Cisco CCNA Discovery

4.0

Forgalomirányítás és kapcsolás nagyvállalati környezetben

(3. szemeszter)

edited by Nono – 2011

1. Vállalati hálózat

1.1 A nagyvállalati hálózatok jellemzői

1.1.1 A vállalat üzleti folyamatainak támogatása

Ahogy nőnek és fejlődnek a vállalkozások, úgy nő a vállalati számítógép-hálózatokkal szembeni elvárás is. Nagyméretű üzleti vállalkozásokként emlegetjük az olyan vállalati környezeteket, melyekhez több telephely, sok felhasználó vagy sok különböző rendszer tartozik. Az alábbiak tipikus nagyméretű üzleti vállalkozási területek:

- Termékgyártók
- Nagykereskedelmi láncok
- Éttermi és szolgáltatói franchise hálózatok
- Állami és közigazgatási szervezetek
- Kórházak
- Iskolarendszerek

A nagyméretű üzleti vállalkozásokat kiszolgáló számítógépes hálózatokat nevezzük nagyvállalati hálózatoknak. A nagyvállalati hálózatoknak számos közös jellemzőjük van. Ilyenek például a következők:

- Kritikus üzleti alkalmazásokat futtatnak
- Konvergált hálózati forgalmat bonyolítanak
- Központosított felügyeletet igényelnek
- Szerteágazó üzleti igényeket elégítenek ki

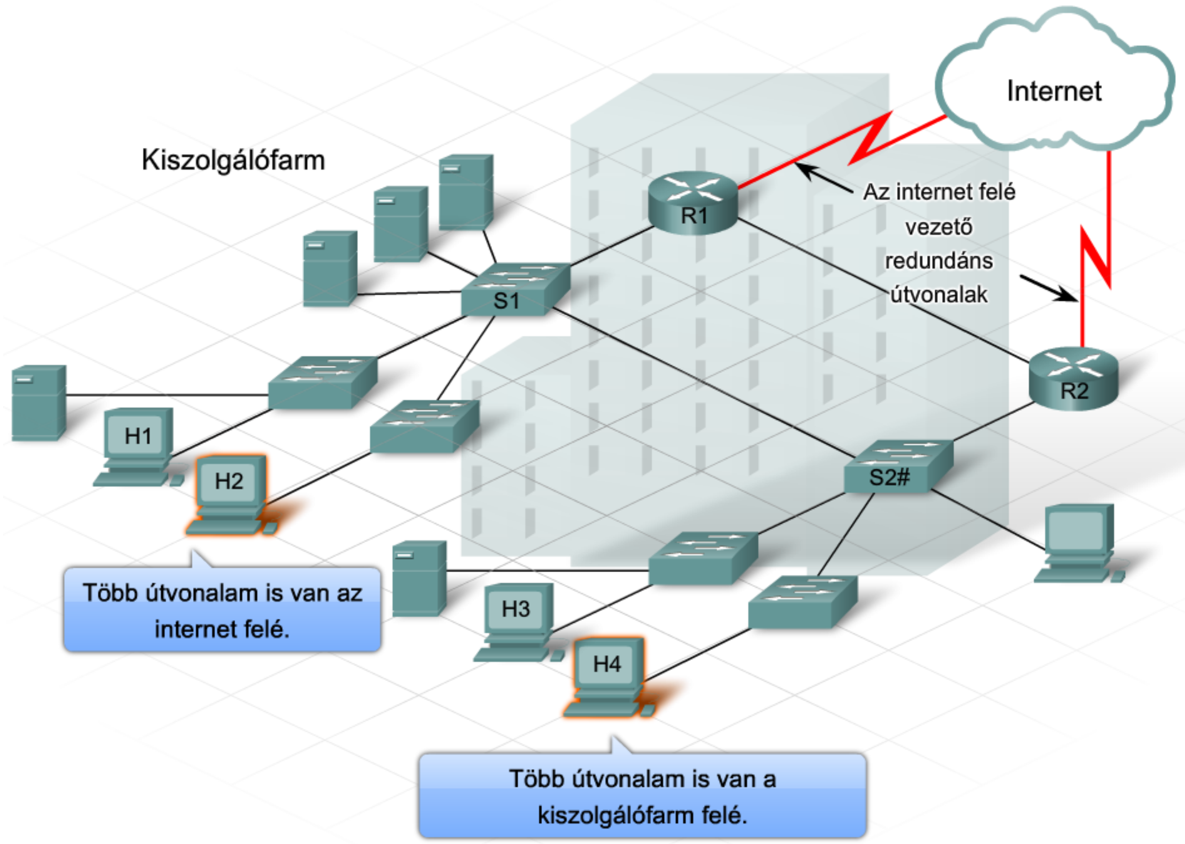
Egy nagyvállalati hálózatnak képesnek kell lennie az egyes üzletrészek közötti olyan egymástól eltérő hálózati forgalomtípusok lebonyolítására, mint például az adatállományok átvitele, elektronikus levelezés, IP telefónia vagy a videó alapú alkalmazások.

Egyre jellemzőbb, hogy a vállalkozások hálózati infrastruktúrájának kritikus üzleti folyamatokat kell kiszolgálnia. A nagyvállalati hálózat leállása ellehetetleníti az üzleti folyamatokat, ami áttételesen bevételkieséshez és a vásárlók elvesztéséhez vezethet. A felhasználók ezért 99,999%-os rendelkezésre állást várnak el a nagyvállalati számítógépes hálózattól.

Az elvárt megbízhatóság teljesítésének érdekében a nagyvállalati hálózatokban magas minőségi kategóriájú eszközöket alkalmaznak. A nagyvállalati piacra szánt eszközöknél elsődleges szempont a megbízhatóság, ezért ezeknek az eszközöknek olyan jellemzőik vannak, mint például a redundáns áramellátás és automatikus hibakezelési képesség. Mivel a nagyvállalati piacra szánt eszközök általában jelentős forgalmat bonyolítanak le, ezért tervezésüket és gyártásukat szigorúbb szabványok szabályozzák mint a szélesebb körben használt eszközökét.

A professzionális eszközök beszerzése és telepítése ugyanakkor nem helyettesítheti a körültekintő hálózati tervezést. A jó hálózati tervezés egyik legfontosabb célja, hogy minden kritikus hibaforrást megelőzzünk. Ez elsősorban a redundancia biztosításával valósítható meg.

A hálózattervezés további lényeges elemei a sávszélesség-felhasználás optimalizálása, valamint a hálózat biztonságának és teljesítményének garantálása.



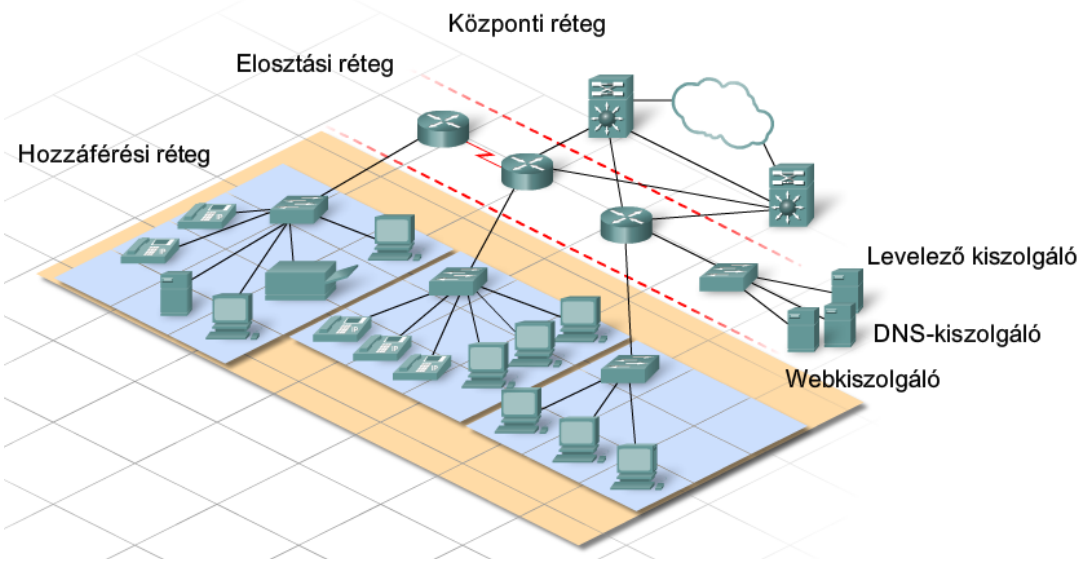
1.1.2 A forgalom alakulása a nagyvállalati hálózatban

A nagyvállalati hálózaton úgy optimalizálhatjuk legjobban a hálózati sávszélesség kihasználtságát, ha úgy alakítjuk ki a hálózatot, hogy a forgalom lehetőleg mindig az adott szegmensen belül maradjon, és ne kerüljön át olyan hálózatszakaszokra, ahova nem szól az üzenet. A háromrétegű, hierarchikus tervezési modell segít a hálózat megfelelő kialakításában. Ez a modell három jól elkülöníthető rétegre osztja a hálózat feladatait: hozzáférési réteg, elosztási réteg és központi réteg. Mindegyik rétegnek jól meghatározott feladata van.

A hozzáférési réteg a felhasználók számára nyújt hálózati kapcsolatot. Az elosztási réteg a helyi hálózatok közötti adatáramlást biztosítja. Végül, a központi réteg az a nagy sebességű gerinc, ahol az egymástól távoli véghálózatok közti kommunikáció zajlik. Felhasználói forgalom a hozzáférési rétegben keletkezik, és amennyiben szükség van rá, áthaladhat a többi rétegen is.

Bár a hierarchikus modell alapvetően 3 rétegű, a költségek csökkentése érdekében saját központi réteg helyett sok üzleti hálózat használja az internetszolgáltató gerinchálózatát.

1. Vállalati hálózat



Hozzáférési réteg

- Kapcsolódási pontot biztosít a nagyvállalati hálózat végfelhasználói eszközei számára.
- Egy hálózati eszköz, például kapcsoló segítségével lehetővé teszi, hogy több állomás kapcsolódhasson egymáshoz.
- Ugyanazon a logikai hálózaton találhatók.
- Ugyanazon a logikai hálózaton található állomások felé továbbítja a forgalmat.
- Ha a csomag egy másik hálózaton található állomásnak szól, az üzenetet átadja az elosztási rétegnek kézbesítésre.

Elosztási réteg

- Kapcsolódási pontot biztosít a különböző helyi hálózatoknak.
- A helyi hálózatok közti információáramlást szabályozza.
- Biztosítja, hogy az azonos helyi hálózaton található eszközök közti forgalom valóban ne hagyja el a hálózatot.
- Továbbítja a más hálózatokba irányuló forgalmat.
- Biztonsági és hálózatfelügyeleti okokból szűri a bejövő és kimenő forgalmat.
- A hozzáférési rétegnél erőteljesebb kapcsolókat és forgalomirányítókat használ.
- Ha a célhálózat nem kapcsolódik közvetlenül, akkor átadja az adatokat a központi rétegnek kézbesítésre.

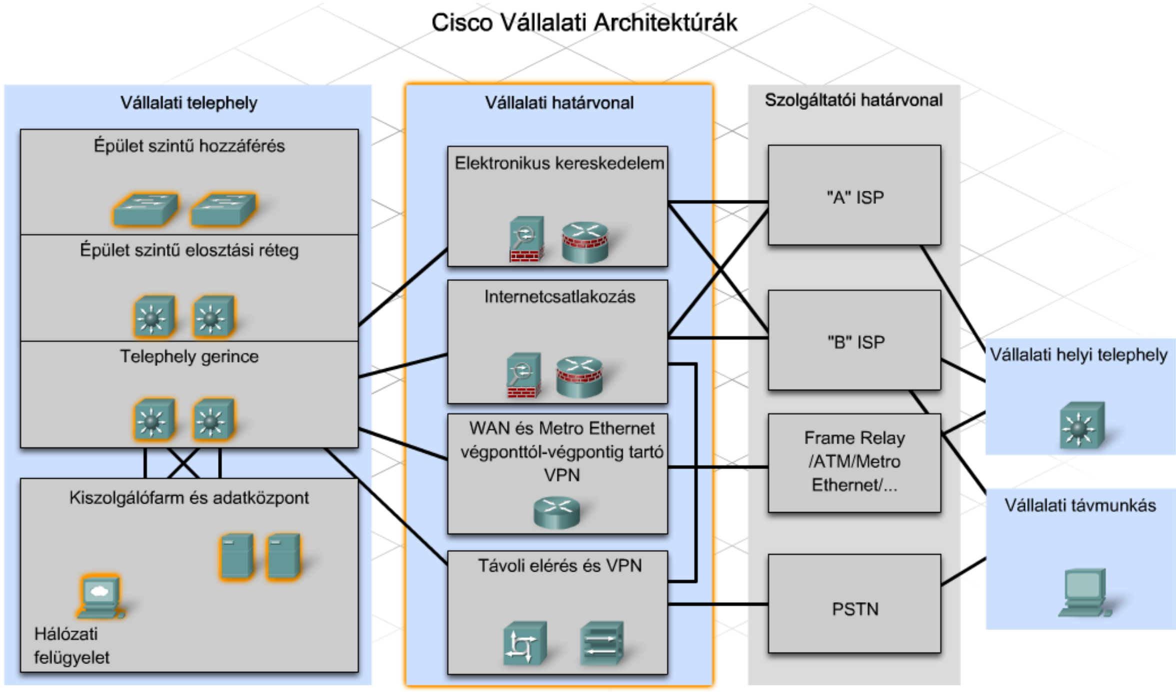
Központi réteg

- Redundáns (tartalék) kapcsolatokat tartalmazó, nagy sebességű gerincet alkot.
- Nagy mennyiségű adatot szállít a számos véghálózat közt.
- Igen erőteljes, nagy sebességű kapcsolókból és forgalomirányítókból áll.

A Cisco Enterprise Architectures (Cisco Vállalati Architektúrák) koncepció úgy bontja fel a hálózatot funkcionális egységekre, hogy közben megtartja a gerinc-, elosztási- és hozzáférési réteg hármas tagolását. A Cisco Enterprise Architectures a következő funkcionális egységeket használja:

- **Vállalati telephely** (Enterprise Campus): A hálózati infrastruktúrát, a kiszolgálófarmot és a hálózati menedzsmentszolgáltatást tartalmazza
- **Vállalati határvonal** (Enterprise Edge): Az internet, a VPN és a WAN modulok összessége, melyek a vállalat hálózatát összekapcsolják a szolgáltató hálózatával.
- **Szolgáltatói határvonal** (Service Provider Edge): Internet-, nyilvános kapcsolt telefon- (PSTN – Public Switched Telephone Network) és WAN szolgáltatásokat nyújt.

Minden az ECNM (Enterprise Composite Network Model – Összetett vállalati hálózatmodell) modellbe belépő vagy kilépő adat a határeszközökön halad keresztül. Ez az a pont, ahol minden csomagot meg lehet vizsgálni, és el lehet dönteni, hogy az adott csomag beengedhető-e a vállalati hálózatba. A rosszindulatú tevékenység kiszűrését elvégző behatolás-érzékelési (Intrusion Detection System – IDS) és behatolás-védelmi (Intrusion Prevention System – IPS) rendszereket is a vállalat határára érdemes telepíteni.



Épületszintű hozzáférés:

Ez a hozzáférési réteg 2. rétegbeli vagy 3. rétegbeli kapcsolókkal valósítja meg a szükséges portsűrűséget. Itt kerülnek megvalósításra a VLAN-ok és az épület elosztási rétege felé vezető trönkvonalak. Az épület elosztási rétegében elhelyezett kapcsolók fontos jellemzője a redindancia.

Épület szintű elosztási réteg:

Ez az elosztási rétegbeli modul 3. rétegbeli eszközökkel valósítja meg az épület szintű hozzáférést. Ebben a rétegben kerül megvalósításra a forgalomirányítás, a hozzáférés-vezérlés és a szolgáltatásminőség (QoS). A redundancia elengedhetetlen ebben a rétegben is.

Telephely gerince:

Ez a gerincrétegbeli modul nagy sebességű kapcsolatot biztosít az elosztási réteg modulja, az adatközpont kiszolgálófarmja és a vállalati határvonal között. Ebben a rétegben a redundancia, a gyors konvergencia és a hibatűrés áll a tervezés középpontjában.

Kiszolgálófarm:
Ez a modul biztosítja a gyors kapcsolatot és a védelmet a kiszolgálóknak. Ezen a területen a biztonság. a redundancia és a hibatűrés a legfontosabb,

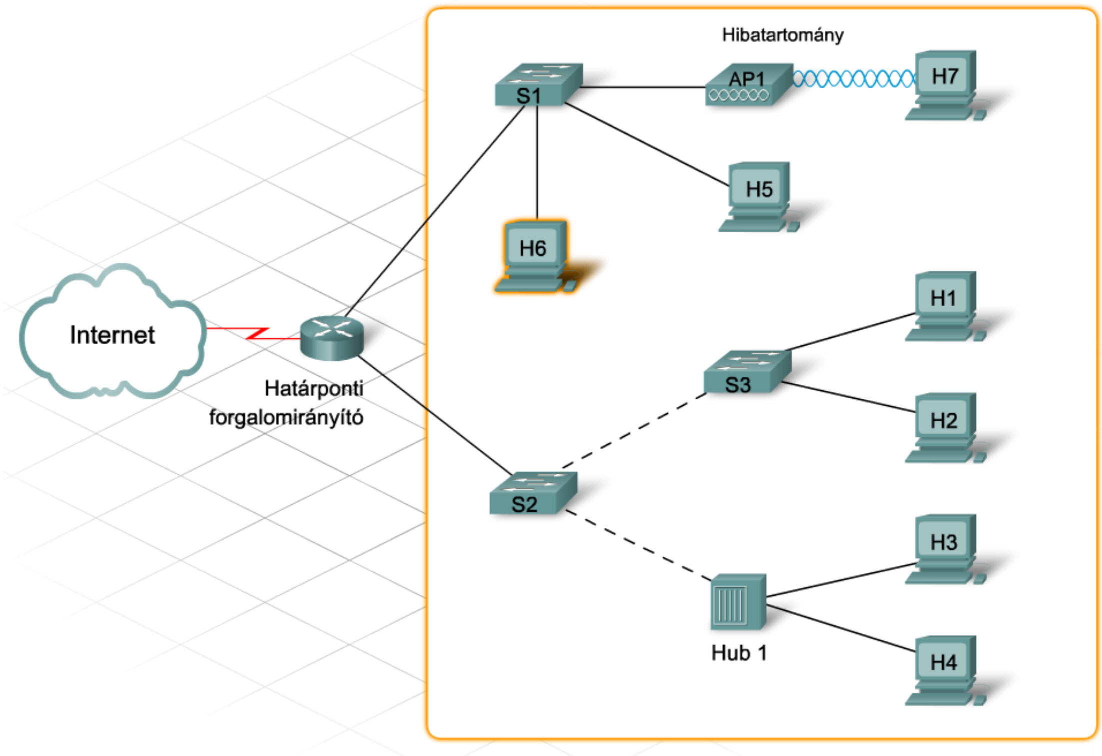
Felügyelet:
Ez a fontos terület felügyeli a teljesítményt azáltal, hogy monitorozza az eszközöket és a hálózati elérhetőségeket.

Vállalati határvonal:
Ez a modul terjeszti ki a vállalati szolgáltatásokat a távoli webhelyek felé és teszi lehetővé, hogy a vállalat elérje az internetet és a partnerek szolgáltatásait. Ez a modul biztosítja a szolgáltatásminőséget (QoS), a hálózati szabályok betartását, a szolgáltatási szinteket és a biztonságot.

Egy jól megtervezett hálózat a forgalom megfelelő szűrése mellett képes a meghibásodások által érintett tartományok minimalizálására is. A hibatartomány az a hálózatszakasz, melyet közvetlenül érint egy kulcsfontosságú hálózati eszköz vagy szolgáltatás meghibásodása.

Az elsőként meghibásodó összetevő nagyban meghatározza, hogy mekkora tartományra lesz hatással a hiba. Például, ha egy adott szegmens kapcsolója hibásodik meg, akkor általában csak az adott szegmens állomásai érintettek. Ugyanakkor, ha az adott szegmenst a többihez kapcsoló forgalomirányító hibásodik meg, akkor sokkal drámaiabb lehet a hatás.

A hálózati károk csökkenthetők redundáns kapcsolatok és megfelelő minőségű, professzionális eszközök használatával. A kisméretű meghibásodási tartományok csökkentik a meghibásodások vállalati termelékenységére gyakorolt hatását, egyszersmind egyszerűsítik a hibaelhárítást, ezáltal csökkentik az egyes felhasználók által tapasztalt leállási időt.



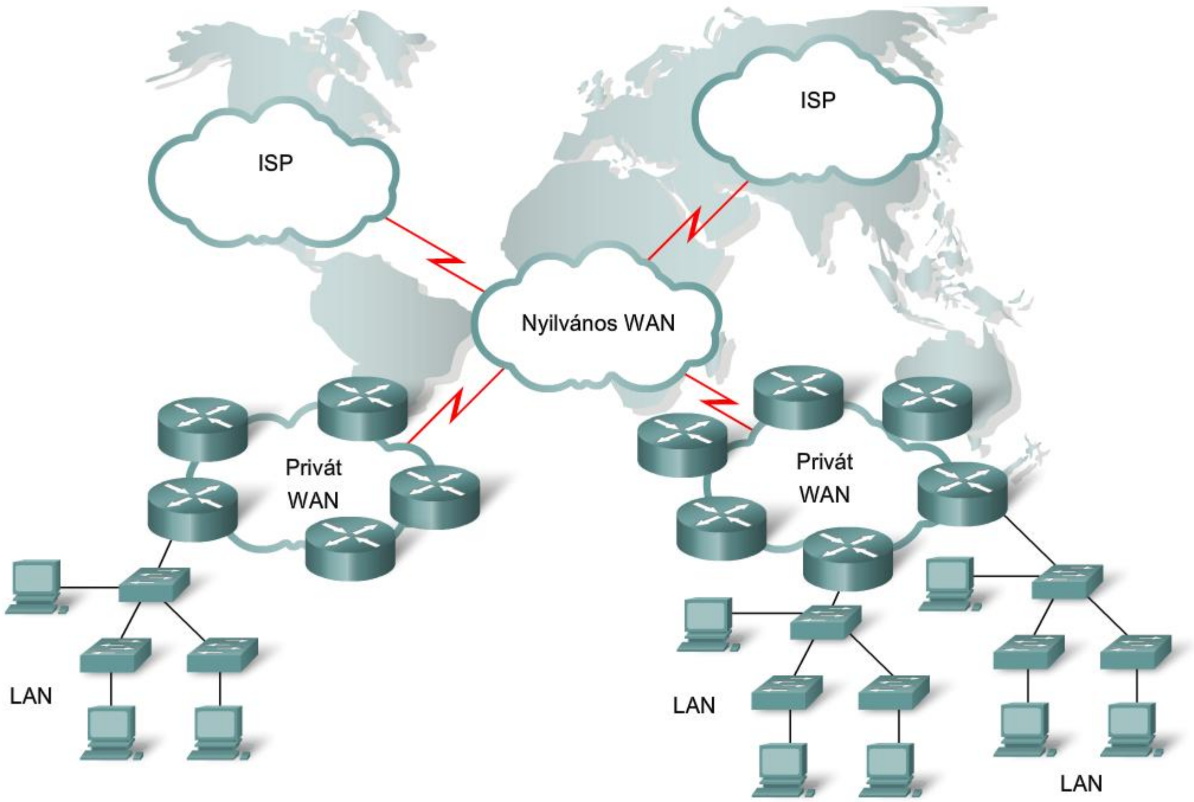
1.1.3 Vállalati LAN-ok és WAN-ok

A vállalati hálózatok általában hagyományos LAN és WAN technológiákat is alkalmaznak. Egy tipikus vállalati hálózatban egyetlen kiterjedt telephely számos helyi hálózata kapcsolódik egymáshoz az elosztási vagy a központi rétegen keresztül, létrehozva így a vállalati LAN-t. Ezek a helyi hálózatok kapcsolódnak aztán a földrajzilag távolabb levő hálózatokhoz, kialakítva egy WAN-t.

A LAN-ok privát hálózatok, egyetlen ember vagy szervezet felügyelete alatt. Ez a szervezet telepíti, felügyeli és gondozza a teljes vezetékezést és a LAN funkcionális építőkövetit képező eszközöket.

Léteznek magánkézben levő WAN-ok is. Mivel a WAN-ok kiépítési- és fenntartási költségei meglehetősen magasak, ezért általában csak igen nagy vállalatok engedhetik meg maguknak, hogy saját WAN-t tartsanak fenn. A legtöbb cég internetszolgáltatótól (ISP – Internet Service Provider) vásárolja a WAN kapcsolatát, így aztán az ISP felel a LAN-ok közti hálózati szolgáltatásokért és a WAN végpontok gondozásáért.

Amikor egy szervezethez sok egymástól távoli telephely tartozik, a WAN kapcsolatok és szolgáltatások kialakítása igen összetetté válhat. Előfordulhat, hogy a vállalat fő internetszolgáltatója nem nyújt minden telephelyen vagy országban szolgáltatást, ahol a vállalatnak irodája van. Ez oda vezethet, hogy a vállalat több különböző internetszolgáltatótól kénytelen szolgáltatást vásárolni. A különböző internetszolgáltatóktól vásárolt szolgáltatások minőségében komoly eltérések lehetnek. Számos feltörekvő ország esetén tapasztalhat a hálózattervező például markáns különbségeket az elérhető eszközök, a kínált WAN szolgáltatások és az adatbiztonságot megvalósító titkosítási technológiák terén. A vállalati hálózat támogatása szempontjából lényeges, hogy az eszközözök, a konfiguráció és a szolgáltatások egységes szabványokat kövessenek.

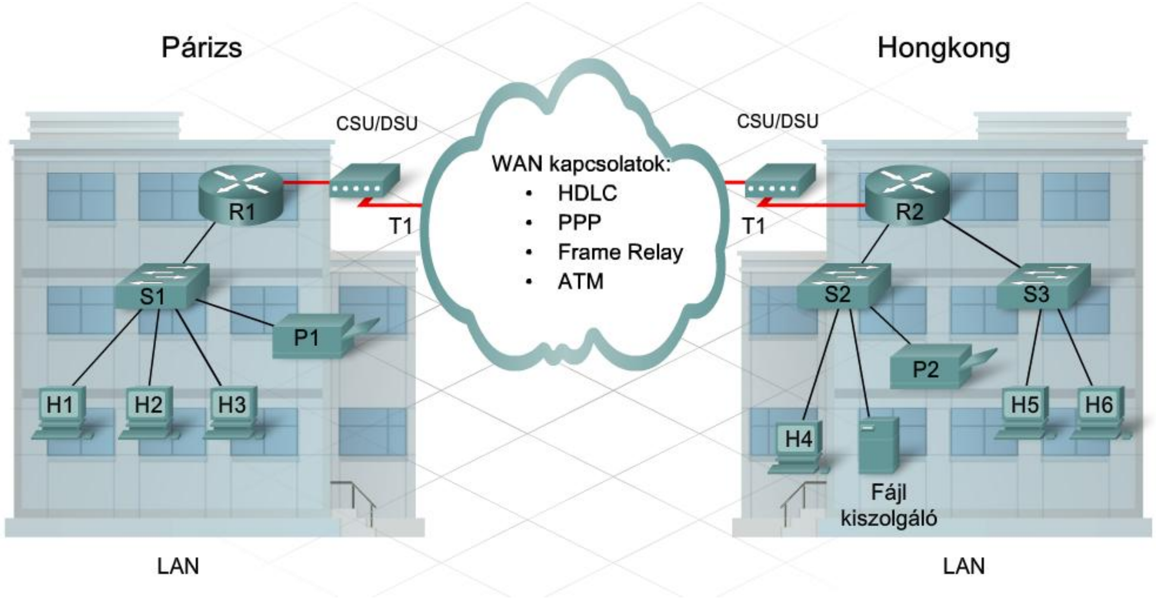


A LAN jellemzői:

- Az üzemeltető szervezet felelős az infrastruktúra kialakításáért és felügyeletéért.
- Az Ethernet a leggyakrabban alkalmazott technológia.
- A hálózat jellemzően a hozzáférési- és az elosztási rétegre fókuszál.
- A LAN biztosítja a felhasználók kapcsolódását, valamint helyi alkalmazások és kiszolgálófarmok elérését.
- Az összekapcsolt eszközök jellemzően egy behatárolt területen – például egy épületen vagy egy nagyobb telephelyen – belül helyezkednek el.

A WAN jellemzői:

- Az összekapcsolt telephelyek földrajzilag távol helyezkednek el egymástól.
- A WAN-hoz történő csatlakozás külön eszköz – modem vagy CSU/DSU – használatát igényelheti, amely lehetővé teszi az adatok szolgáltatói hálózatnak megfelelő formátumra alakítását.
- A szolgáltatásokat az ISP nyújtja. A tipikus WAN szolgáltatások közé tartozik a T1/T3, az E1/E3, a DSL, a kábel-TV alapú internet, a Frame Relay és az ATM.
- Az infrastruktúra kialakítása és felügyelete az ISP feladata.
- A határeszközök alakítják át az Ethernet beágyazást soros WAN beágyazássá.



1.1.4 Intranetek és extranetek

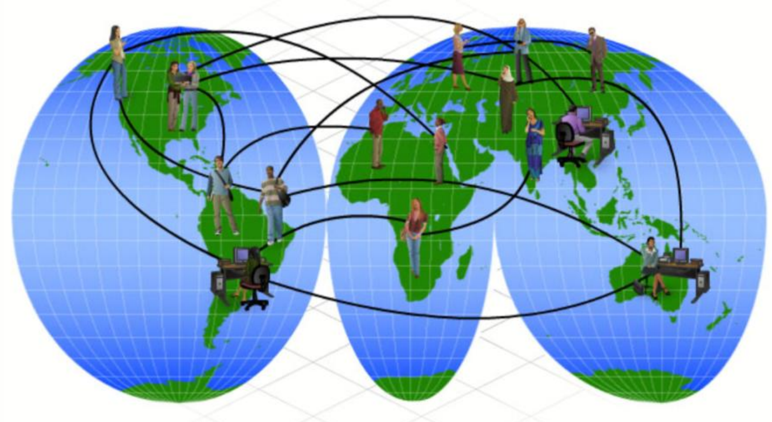
A vállalati hálózatok LAN és WAN technológiákat is alkalmaznak. Ezek a hálózatok számos olyan szolgáltatást is nyújtanak, melyeket jellemzően az internethez szoktunk kapcsolni. Ilyen szolgáltatások például az alábbiak:

- E-mail
- Web
- FTP
- Telnet/SSH
- vitafórumok

1. Vállalati hálózat

A cégek jellemzően ezen a privát hálózaton vagy intraneten keresztül biztosítják a helyi és a távoli alkalmazottaiknak az elérést LAN és WAN technológiák alkalmazásával.

Az intranetek kapcsolódhatnak az internethez is, ilyenkor általában tűzfal felügyeli az intranetre belépő és onnan kilépő forgalmat.



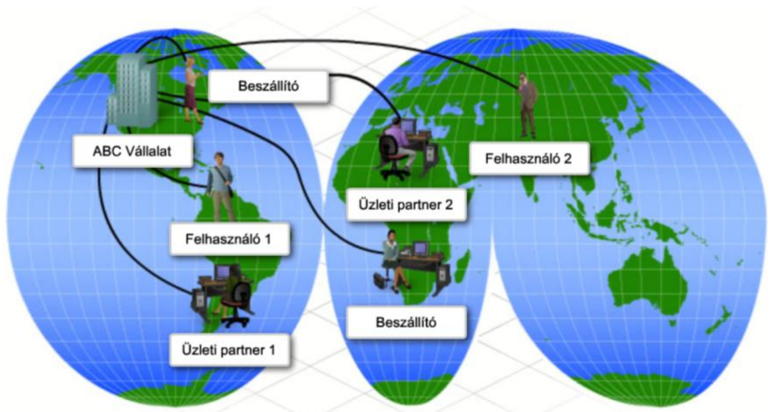
Nagyvállalati intranet
A vállalat alkalmazottai a világ legkülönbözőbb pontjairól csatlakoznak az intranethez.

Az intranetek általában bizalmas információkat tartalmaznak, és kizárólag a vállalat alkalmazottai számára vannak kialakítva. Az intranetet minden esetben tűzfallal kell védeni. Azok a távolról dolgozó alkalmazottak, akik nem közvetlenül kapcsolódnak a vállalati LAN-hoz, hitelesítést követően kaphatnak hozzáférést.

Bizonyos esetekben a vállalkozások kiterjeszthetik hálózatuk elérését a kiemelt ügyfeleik és beszállítóik számára. Ennek leggyakoribb megoldásai:

- Közvetlen WAN kapcsolat
- Kulcs-alkalmazásoktávoli belépéssel történő elérése
- VPN kapcsolódás a védett hálózathoz

Extranetnek hívjuk az olyan intranetet, ami külső kapcsolódást biztosít a vállalat beszállítói és más szerződéses partnerei számára. Az extranet tehát egy olyan privát hálózat (intranet), amely szervezeten kívüli egyének és társaságok számára biztosít ellenőrzött hozzáférést. Az extranet nem nyilvános hálózat.



Nagy méretű vállalati extranet
Kiemelt beszállítók és üzleti partnerek, akiknek ellenőrzött hozzáférésük van a vállalati intranethez.

1.2 A vállalati alkalmazások azonosítása

1.2.1 Forgalomáramlási mintázatok

A megfelelően megtervezett vállalati hálózatokat jól definiált, kiszámítható forgalmi mintázat jellemzi. Bizonyos körülmények között a hálózati forgalom a vállalati LAN területére korlátozódik, máskor kilép onnan a WAN kapcsolatokon keresztül.

A hálózat megtervezésének egyik fontos szempontja, hogy meghatározzuk az egyes célterületek felé irányuló forgalom mértékét és forrását. Az alábbi forgalomtípusoknak például alapvetően a felhasználók hálózatán belül kell maradnia:

- fájlmegosztás
- nyomtatás
- belső biztonsági mentés és adattükrözés
- telephelyen belüli hangátvitel

Más forgalomtípusok előfordulhatnak a hálózaton belül és a WAN kapcsolatokon is. Ilyenek például az alábbiak:

- rendszerfrissítések
- vállalati elektronikus levelezés
- tranzakció-feldolgozás

A WAN kapcsolati forgalom mellett külső forgalomnak számít az internetről származó, vagy oda irányuló forgalom is. A VPN és az internet adatforgalom egyértelműen külső forgalom.

Az adatforgalom szabályozása optimalizálja a hálózati sávszélesség felhasználását, továbbá azáltal, hogy monitorozási lehetőséget biztosít, hozzájárul az alapfokú adatbiztonság megvalósításához is. A hálózati forgalmi minták és folyamatok elemzése révén a rendszergazda megítélheti a várható forgalom típusát és mértékét. Az olyan forgalom, ami nem várt helyen jelentkezik a hálózatban, kiszűrhető és forrása is ellenőrizhető.

1.2.2 Alkalmazások és forgalom vállalati hálózaton

Volt idő, amikor az adatok, a hang- és a videó- információk külön-külön hálózatokon utaztak. A mai technológiával megvalósítható olyan összevont hálózat, ahol az adat-, a hang- és a videó-jeleket egyazon közegen továbbítjuk.

Az összevonás számos tervezési és sávszélesség-gazdálkodási kihívást jelent. A vállalati hálózat a legkülönfélébb alkalmazásoktól származó forgalom-összetevők továbbitásával elégíti ki a vállalat igényeit. Ilyen forgalom-összetevőkaz alábbiak:

- Adatbázis-tranzakciók
- Nagygép, illetve adatközponti elérés
- Állomány- és nyomtatómegosztás
- Hitelesítés
- Webszolgáltatások
- E-mail és egyéb kommunikációk

- VPN szolgáltatások
- Hanghívások és hangüzenetek
- Videó és videokonferencia

Mindezek mellett a hálózat üzemeltetése és a hálózat működéséből fakadó folyamatok is hálózati erőforrásokat igényelnek.

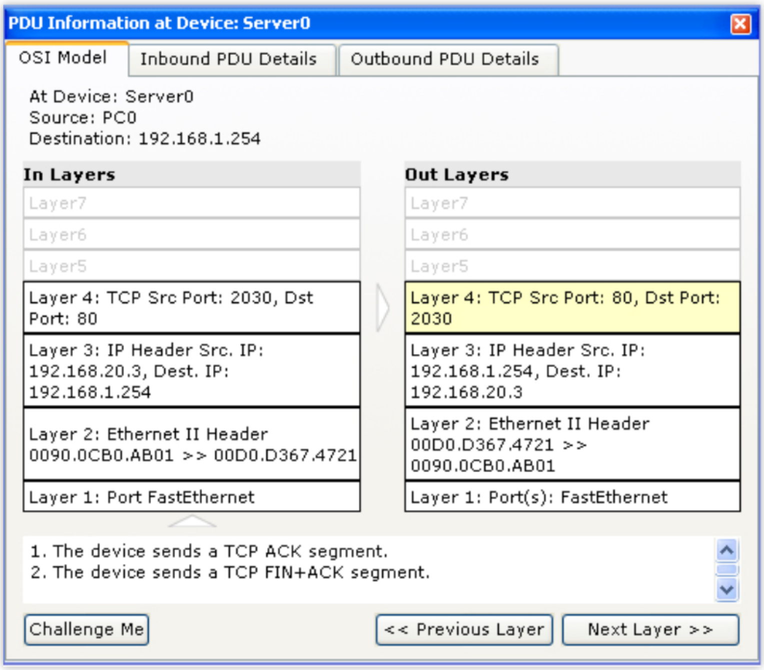
A hálózati folyamat menedzselésének megtervezése szempontjából elsődleges fontosságú a hálózaton zajló forgalom és adatáramlási folyamatok megértése. Ha nem ismerjük a hálózati forgalom összetevőit, akkor a forgalom, további elemzés céljából, csomagvizsgáló alkalmazással rögzíthető.

A hálózati forgalmi minták megismerése érdekében fontosak az alábbiak:

- Mindig a forgalmi csúcs közelében rögzítsük a csomagokat, így megfelelően jó mintát nyerhetünk a különböző típusú forgalmakból!
- Mivel bizonyos forgalomtípusok adott helyhez köthetőek, mindig vegyünk mintát több hálózatszakaszról is!

A csomagvizsgáló alkalmazással gyűjtött minták alapján meghatározhatók a forgalmi folyamatok. A minta elemzése során a hálózati technikus elsősorban a megvizsgált csomagok forrás- és célcímére, valamint a forgalmi típusokra alapozva vonhat le következtetéseket. Az elemzés alapján hozhatók meg azok a döntések, melyekkel hatékonyabbá tehető a hálózati forgalom menedzselése. Célszerű lehet például a felesleges forgalom csökkentése, vagy a teljes forgalmi minta átalakítása egy kiszolgáló áthelyezésével.

Sokszor egyetlen kiszolgáló, vagy szolgáltatás másik hálózati szakaszba való áthelyezése önmagában javíthatja a hálózat teljesítményét. Máskor azonban csak a hálózat újratervezésével vagy komolyabb beavatkozással lehet a hálózati teljesítményt optimalizálni.



1.2.3 Prioritások a hálózati forgalomban

A hálózaton megfigyelhető különböző forgalomtípusok eltérő jellemzőkkel, igényekkel és viselkedéssel bírhatnak.

Adatforgalom

A legtöbb hálózati alkalmazás adatforgalmat generál. Egyes alkalmazások rendszertelen időközökben küldenek adatokat, míg mások (például az adattárházak) hosszabb időn át jelentős mennyiségű adatot továbbítanak.

Vannak adatalkalmazások melyek érzékenyebbek az időtényezőre, mint a megbízhatóságra, de többségük jól tolerálja a késést. A fentiek miatt a legtöbb adatalkalmazás a TCP (Transmission Control Protocol – átvitelvezérlési protokoll) protokollt használja. A TCP protokoll nyugták alkalmazásával követi, hogy újra kell-e valamelyik csomagot küldeni, ezáltal garantálja a megbízható átvitelt. A nyugták alkalmazása amellett, hogy megbízhatóvá teszi az átvitelt, késletetést is okoz.

Hang- és videó átvitel

A hang- és videó forgalom alapvetően különbözik az adatforgalomtól. A hang- és videóátvitel zökkenőmentes adatfolyamot követel a jó hang- és képminőség érdekében. A TCP protokoll nyugtázási technikája késéseket okoz, ami megtöri az adatfolyamot, és ezáltal rontja az alkalmazás minőségét. Ezért a hang- és videó alkalmazások általában az UDP (User Datagram Protocol – felhasználói datagram protokoll) protokollt használják a TCP helyett. Mivel az UDP nem tartalmaz a csomagok újraküldését biztosító eljárást, így csak minimális késést okoz.

A TCP és UDP protokollok okozta késésbeli különbségek megértése mellett fontos látni, hogy a hálózati eszközök is késleltetést okoznak, miközben a továbbításhoz feldolgozzák a csomagokat. Az OSI modell 3. rétegéhez tartozó eszközök nagyobb késleltetést okoznak, mint a 2. réteghez tartozók, mivel több fejrész-információt kell feldolgozniuk. Ennek megfelelően a forgalomirányítók okozta késleltetés például nagyobb, mint a kapcsolók által okozott.

A hálózati torlódás miatti késleltetési bizonytalanság (jitter) az a jelenség, amikor az egyes csomagok váltakozó hosszúságú idő alatt érnek el a célhoz.

Időzítés-érzékeny forgalom esetén fontos cél a késleltetés és a késleltetési bizonytalanság hatásait minél jobban csökkenteni.

A szolgáltatásminőség (Quality of Service – QoS) olyan folyamat, ami egy adott adatfolyam számára minőségi garanciákat biztosít. A QoS folyamat prioritások alapján sorokba rendezi a forgalmat. A hangátvitel például prioritást élvez a hagyományos adatokkal szemben.



Osztályozás

A különböző alkalmazásoktól származó adatok a forgalomirányító kimenő interfésze felé haladnak.

Kattintson a **Lejátszás** gombra az animáció folytatásához!



Várósorba kerülés előtt

A forrásalkalmazásuk alapján osztályozott adatok: videó, hang, FTP forgalom stb.

A piros elemek jelölik a nem kívánatos forgalmat, melyek kiszűrésre kerülnek.

Kattintson a **Lejátszás** gombra az animáció folytatásához!



Várósorok és időzítés

A forgalom előre beállított prioritások alapján kerül a várósorokba. A magas prioritású sorok (például P1, P2) csomagjai előbb lesznek továbbítva, mint az alacsony prioritású soroké (például P5, P6).

Példa: a hanginformáció nem tolerálja a késleltetést, ezért a magas prioritású sorba kerül, így elsőként lesz továbbítva.

Kattintson a **Lejátszás**

1.3 Távoli alkalmazottak támogatása

1.3.1 Telefonos távmunka

A nagyvállalati hálózatok és a távolról történő csatlakozást biztosító technológiák fejlődése alapjaiban változtatta meg mindennapi munkavégzésünket.

A telefonos távmunka, más nevén e-munkavégzés, lehetővé teszi, hogy a munkavállalók a különböző telekommunikációs lehetőségeket kihasználva otthonról, vagy más, munkahelyüktől távoli helyszínről végezzék munkájukat. Az ilyen, távolról dolgozó munkatársat nevezzük távmunkásnak.

Egyre több vállalat bíztatja munkatársait otthoni munkavégzésre. A távmunka számos előnnyel járhat mind a munkaadó, mind a munkavállaló részére. A munkaadó szemével nézve a távmunkás kolléga részére nem kell saját fizikai helyet biztosítani az irodában, így elegendő egyetlen közös munkahelyet kialakítani, ahol az éppen az irodában tartózkodó munkatárs helyet tud foglalni. Ez a megoldás jelentős mértékben csökkentheti az irodai ingatlan- és fenntartási költségeket.

Egyes cégek még a repülőjegyekre és hoteléjszakákra fordított költségeiket is úgy csökkentik, hogy telekonferenciával és más kollaborációs eszközökkel hozzák össze munkatársaikat. A világ legkülönbözőbb pontjain tartózkodó emberek dolgozhatnak ezáltal úgy, mintha egy helyen tartózkodnának.

A munkavállaló és a munkaadó is egyformán jól jár a távmunkával.

A munkavállaló időt és pénzt takarít meg, ráadásul nem terheli a napi utazgatással együtt járó stressz. Otthonukban kiöltözniük sem kell, így további pénzt takaríthatnak meg a munkaöltözeten. Otthon dolgozva a munkavállalók több időt tölthetnek családjukkal.

A kevesebbet utazó munkavállaló a környezetet is jobban kíméli. A kisebb repülőgépes és autóforgalom kevesebb légszennyezést jelent.

A távmunkásnak persze önállónak és fegyelmezettnek kell lennie. Egyes távmunkások hiányolják a munkahelyi közösséget, és nem szeretnek elszigetelten dolgozni.

Vannak munkakörök, melyekben nem előnyös a távmunka. Egyes pozíciók egyszerűen igénylik az adott idősávban a személyes irodai jelenlétet. Mégis egyre több vállalkozás és mind gyakrabban él a technológia biztosította e-munkavégzés lehetőségével.

A hatékony távmunka megvalósításának vannak eszközszükségletei. Ilyenek például az alábbiak:

- Elektronikus levelezés
- Csevegés
- Munkaasztal- és alkalmazás-megosztás
- FTP
- Telnet
- VoIP
- Videokonferencia



Videokonferencia
Lehetővé teszi, hogy távoli helyeken tartózkodó résztvevők szemtől-szembe, egymást látva beszélgethessenek.

E-mail
Lehetővé teszi egy írott üzenet eljuttatását egy távoli felhasználóhoz, aki később válaszolni tud arra.

Azonnal üzenetküldő alkalmazás
Lehetővé teszi azonnali üzenetek valóidejű küldését a távoli felhasználónak, aki rögtön tud azokra válaszolni.

Alkalmazás-megosztás
Lehetővé teszi, hogy egyszerre több felhasználó is ugyanazt az alkalmazást használja.

FTP
Fájlátvitelt tesz lehetővé számítógépek között.

Telnet
Távoli kapcsolódást és terminálkapcsolatot biztosít távoli eszközökhöz.

VoIP
Valós idejű beszélgetést tesz lehetővé internetes technológiák alkalmazásával.

Az alkalmazások és a képernyő megosztására szolgáló segédeszközök rengeteget fejlődtek, ma már egyidejű hang- és videó átvitelre is képesek.

Az új technológia egyre kifinomultabb együttműködést tesz lehetővé. A vállalati hálózat segítségével ez a technológia olyan környezetet teremt az egymástól távol tartózkodó munkatársak számára, mintha egy szobában ülnének. Nagy kivetítők, és jó minőségű hangrendszer alkalmazásával egy speciálisan kialakított teremben az egész hatás olyan lehet, mintha az összes résztvevő – függetlenül a tényleges tartózkodási helyüktől – ott ülne egyetlen tárgyalóasztal körül.

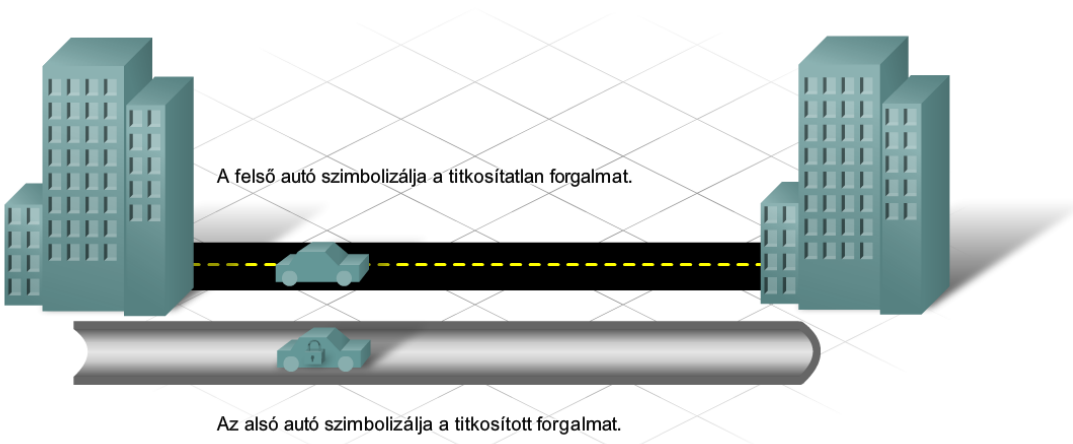
Az ábrán látható társaságból csak az előtérben ülő 5 ember van valójában jelen a szobában. A képernyőkön megjelenő másik 4 személy igazából 3 másik helyszínen tartózkodik.

1.3.2 Virtuális magánhálózatok

A távmunkások által leggyakrabban megtapasztalt nehézség a távmunkához használatos eszközök adatbiztonsági problémája. A nem biztonságos eszközök használata miatt a továbbított információ lehallgatható vagy módosítható.

Egy lehetséges megoldás a problémára, ha az adott feladatot ellátó alkalmazások közül a biztonságos átvitelt alkalmazó változatokat használjuk. Telnet helyett például használjunk SSH klienst! Sajnos nem minden esetben áll rendelkezésre biztonságos alkalmazás, így sokkal kézenfekvőbb megoldás, hogy titkosítsunk minden forgalmat a távoli helyszín és a vállalati hálózat között virtuális magánhálózatot használva (VPN – Virtual Private Network).

A VPN-eket szokás alagútnak (angolul tunnel) is nevezni. A hasonlóság megértéséhez gondolatban hasonlítsuk össze két pont között a földalatti alagút és a földfelszíni nyilvános útvonal lehetőségeit! Minden, ami az alagutat használja a két pont között, az védve van, és láthatatlan. Itt az alagút jelképezi a VPN beágyazást és a virtuális alagutat.



VPN használatakor virtuális alagút jön létre a forrás és a cél között. A forrás és a cél közti összes kommunikációt titkosítja a biztonságos beágyazást használó protokoll. Ez a biztonságos csomag kerül továbbításra a hálózaton. A célállomáshoz megérkezve a csomagot kicsomagolják és visszaállítják a titkosítatlan tartalmat.

A VPN megvalósítások ügyfél/kiszolgáló alapúak, így a távmunkásnak először telepítenie kell a VPN kliensprogramot a számítógépére, amivel aztán ki tudja alakítani a biztonságos kapcsolatot a vállalati hálózat irányába.

A VPN technológiával kapcsolódó távmunkások gyakorlatilag részei lesznek a vállalati hálózatnak, hozzáférnek az összes szolgáltatáshoz és erőforráshoz, mintha csak fizikailag is a LAN-hoz kapcsolódnának.

A VPN hálózatok egyik leggyakrabban használt beágyazási protokollja az IPSec, ami az IP Security (IP biztonság) angol kifejezés rövidítése. Az IPSec valójában egy számos szolgáltatást nyújtó protokollcsomag. Ilyen szolgáltatások például: adattitkosítás, integritás-ellenőrzés, társak hitelesítése. kulcskezelés.

1.4 A fejezet összefoglalása

- Nagyméretű üzleti vállalkozásokként emlegetjük az olyan vállalati környezeteket, melyekhez több telephely, sok felhasználó vagy sok különböző rendszer tartozik.
- A nagyvállalati hálózatok szolgálják ki a vállalat számára létfontosságú alkalmazásokat, a hálózati forgalmat, központosított felügyeletet valósítanak meg, miközben a legkülönbözőbb gazdasági elvárásoknak kell megfelelniük.

A nagyvállalati hálózat:

- 99,999% rendelkezésre állást biztosít.
- LAN és WAN összetevőket is használ.
- Számos különböző technológiát alkalmaz.
- Valamelyik internetszolgáltató (ISP) szolgáltatását használja.
- Különböző típusú adatforgalmakat bonyolít, többek között: hang-, videó- és adatforgalmat.
  - Vállalati telephely (Enterprise Campus): A kiszolgálófarmot és a hálózati menedzsmentszolgáltatást tartalmazó infrastruktúra.
  - Vállalati határvonal (Enterprise Edge): Az internet, a VPN és a WAN modulok összessége, melyek a vállalat hálózatát összekapcsolják a szolgáltató hálózatával.
  - Szolgáltatói határvonal (Service Provider Edge): Internet-, nyilvános kapcsolt telefon- (PSTN – Public Switched Telephone Network) és WAN szolgáltatásokat nyújt.
  - Hibatartomány (Failure Domain): azon eszközök halmazát jelöli, melyeket egy fontos készülék vagy szolgáltatás meghibásodása érint.
- Az intranet olyan magánhálózat, mely TCP/IP és más technológiák segítségével nyújt magánjellegű szolgáltatásokat a vállalat saját alkalmazottainak.
- Amennyiben a viszonteladók, az egyéb üzleti partnerek és más külső egyének is hozzáférhetnek az intranethez, akkor extranetről beszélünk.
- A hálózati forgalmat tartsuk azon a hálózatszakaszon, ahova az szól!
- A forgalom egy része áthalad a vállalati WAN-on, más része kijut a vállalati hálózatról is.
- A QoS szolgáltatás lehetővé teszi, hogy bizonyos forgalmat előnyben részesítsünk a többivel szemben, például a hang- és videoátvitel előnyt élvezhet az adatátvitellel szemben.
- A telekommunikációs távmunka technológiai megoldásokkal helyettesíti az üzleti utakat.
- A munkavállaló, a munkaadó és még a környezet is egyformán jól jár a távmunkával.
- A technológia fejlődésével egyre több munkakör esetén lesz alkalmazható a távmunka.
- A távmunkás munkavégzését olyan eszközök segítik, mint az elektronikus levelezés, a csevegés, az alkalmazás- és munkafelület-megosztás, az FTP, a telnet, a VoIP és a videokonferencia.
- A VPN titkosított csatornákat hoz létre a különböző telephelyek között, ezáltal megoldást nyújt a távmunkások biztonsági elvárásaira.

2. A vállalatok hálózati infrastruktúrájának megismerése

2.1 Az aktuális hálózat leírása

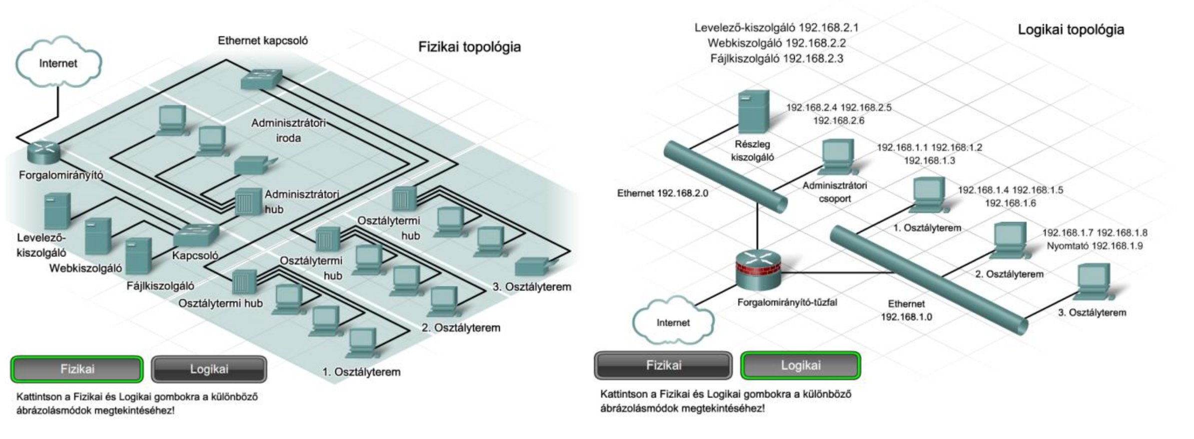
2.1.1 A vállalatok hálózati dokumentációja

Ha egy hálózati szakember új helyen kezd dolgozni, akkor először meg kell ismerkednie a hálózat jelenlegi felépítésével. Egy vállalati hálózat állomások ezreiből és hálózati eszközök százaiból állhat, amelyek réz, optikai vagy vezeték nélküli technológiával kapcsolódnak egymáshoz. Az összes végfelhasználói munkaállomásról, kiszolgálóról és hálózati eszközről (pl. kapcsolókról és forgalomirányítókról) dokumentációt kell vezetni. A dokumentációk számos típusa létezik, ezek mind más-más szemszögből mutatják be a hálózatot.

A hálózatszerkezeti diagram vagy másképpen topológia diagram nyilvántartja az eszközök helyét, funkcióját és állapotát. Topológia diagram készülhet a hálózat fizikai és logikai felépítéséről egyaránt.

A fizikai topológia rajzán ikonokkal jelölik az állomások, hálózati eszközök és az átviteli közegek helyét. A fizikai topológia rajzát mindig naprakész állapotban kell tartani, hogy segítségünkre lehessen a későbbi telepítési és hibaelhárítási feladatok során.

A logikai topológia rajza a fizikai helyüktől függetlenül, a hálózati összetartozás alapján csoportosítja az állomásokat. A logikai topológia rajzán állomásnevek, címek, csoportinformációk és hálózati alkalmazások megnevezése szerepelhet. A vállalatok hálózati diagramjai hálózatirányítási információkat is tartalmaznak, melyek leírják a hibatartományokat, valamint megadják, hogy mely interfészeknél keresztezik egymást a különböző hálózati technológiák.



Döntő fontosságú, hogy a hálózati dokumentáció naprakész és pontos legyen. A hálózati dokumentáció a hálózat telepítésekor általában még pontosan mutatja az akkori állapotot, de a későbbi növekedését és változásait nem minden esetben követi.

A hálózati topológia rajza rendszerint az eredeti épület-alaprajzokon alapul. Elképzelhető, hogy az alaprajz megváltozott az épület elkészülése óta. A változások megfelelően jelöléssel vagy átrajzolással az eredeti tervrajzon is dokumentálhatók. Az ily módon módosított rajzot megvalósulási

diagramnak nevezzük. Az építés szerinti diagram a tényleges hálózati felépítést dokumentálja, amely eltérhet az eredeti tervektől. Mindig bizonyosodjunk meg arról, hogy a jelenlegi dokumentáció az eredeti alaprajz mellett a hálózati topológia összes változását is tartalmazza!

A hálózati diagram általában grafikus rajzolóprogram segítségével készül. A hálózati diagram készítésére alkalmas programok jelentős része azon kívül, hogy rajzeszközként használható, egy adatbázishoz is kapcsolódik. Ez a funkció lehetővé teszi, hogy a hálózati támogatást végző csapat tagjai részletes dokumentációt készítsenek, amelyben rögzítik az állomások és a hálózati eszközök adatait, beleértve a gyártót, a modellszámot, a vásárlás dátumát, a jótállási időt és más egyéb információkat. Ha a diagramon rákattintunk egy eszközre, akkor az eszköz adatait megjelenítő űrlap nyílik meg.

A hálózati diagramok mellett a vállalati hálózatok számos más, fontos szerepet betöltő dokumentációtípust is használnak.

Üzletfolytonossági terv:

Az üzletfolytonossági terv (Business Continuity Plan, BCP) határozza meg a természeti vagy ember által előidézett katasztrófa esetén az üzletfolytonosság megőrzéséhez szükséges lépéseket.

Üzletbiztonsági terv:

Az üzletbiztonsági terv (Business Security Plan, BSP) tartalmazza a fizikai-, rendszer- és szervezeti szintű adatvédelmi intézkedéseket. Az általános biztonsági tervnek tartalmaznia kell egy informatikai részt, amely leírja, hogy a szervezet hogyan védi a hálózatát és információs értékeit.

Hálózat-karbantartási terv:

A hálózat-karbantartási terv (Network Maintenance Plan, NMP) a hálózat folyamatos és hatékony üzemeltetésével biztosítja az üzletfolytonosságot. A hálózat-karbantartási munkákat konkrét időszakokra (általában éjszakára vagy hétvégére) kell ütemezni, hogy a lehető legkisebb legyen az üzletmenetre gyakorolt hatása.

Szolgáltatási szerződés:

A szolgáltatási szerződés (Service Level Agreement, SLA) az ügyfél és a szolgáltató vagy ISP között létrejött megegyezés, amely olyan tételeket rögzít, mint például a hálózat rendelkezésre állása vagy a problémák kezelésére vállalt válaszidő.

Üzletfolytonossági terv

Egy esetleges katasztrófa során végrehajtandó lépések meghatározásával biztosítja az üzlet működését. Az IT támogatás részét képezheti(k):

- a biztonsági mentések külső helyen történő tárolása
- alternatív IT feldolgozóközpontok
- redundáns kommunikációs kapcsolatok

Üzletbiztonsági terv

A biztonsági irányelvek rögzítésével megakadályozza a szervezeti erőforrásokhoz és értékekhez történő illetéktelen hozzáférést. Az IT biztonsági terv az alábbiakhoz kapcsolódó irányelveket tartalmazhat:

- Felhasználói hitelesítés
- Megengedett szoftverek
- Távoli elérés
- Behatolás-érzékelés
- Eseménykezelés

Hálózat-karbantartási terv

A hardver- és szoftverkarbantartási folyamatok rögzítésével minimalizálja a leállási időt. A karbantartási terv az alábbiakat tartalmazhatja:

- a karbantartási időszakok
- a tervezett leállási idő
- a személyzet felelőssége
- a karbantartandó eszközök és szoftverek (operációs rendszer, IOS, szolgáltatások)
- a hálózati teljesítmény felügyelete

Szolgáltatói szerződés

A szolgáltatótól elvárt teljesítményszint rögzítésével biztosítja a szolgáltatási paramétereket. A szolgáltatási szerződés (SLA) az alábbiakat tartalmazhatja:

- a kapcsolatok sebessége / sávszélessége
- a hálózat rendelkezésre állási ideje
- a hálózati teljesítmény felügyelete
- a problémamegoldás válaszideje
- a felelősség kérdése

2.1.2 A hálózati szolgáltatási központ

A legtöbb vállalati hálózatban létezik az összes hálózati erőforrás központi kezelését lehetővé tevő hálózati szolgáltatási központ (Network Operations Center, NOC). Az ilyen központot néha adatközpontnak is nevezik.

Egy tipikus vállalatnál a hálózati szolgáltatási központ munkatársai a helyi telephely és a távoli helyszínek számára egyaránt nyújtanak támogatást, azaz a helyi feladatokon túl a nagytávolságú hálózatokkal kapcsolatos teendőket is elvégzik. A nagyobb hálózati központok akár több helyiséget is elfoglalhatnak, mivel a hálózati berendezések és a támogatószemélyzet ide koncentrálódik.

A hálózati központ tipikus jellemzői:

- Álpadló biztosítja, hogy a kábelezés és az áramellátás a padló alatt jusson el a berendezésekhez
- Nagyteljesítményű szünetmentes áramforrás és légkondicionáló berendezés biztosítja az eszközök biztonságos üzemeltetését
- Mennyezetbe integrált tűzoltórendszer működik
- Hálózatfigyelő állomások, kiszolgálók, biztonsági mentést végző rendszerek és adattárházak állnak rendelkezésre

- Hozzáférési rétegbeli kapcsolóknak és elosztási rétegbeli forgalomirányítóknak biztosít helyet, ha a központi kábelrendező (Main Distribution Facility, MDF) szerepét is ez tölti be az épületben vagy a telephelyen.



A hálózati támogatáson és a hálózat-felügyeleten kívül számos hálózati központ biztosít központosított erőforrásokat (pl. kiszolgálókat és adattárházakat).

A hálózati központ kiszolgálói általában kiszolgálófarmot alkotó klaszterekbe vannak szervezve. A kiszolgálófarm rendszerint egyetlen erőforrásnak tekinthető, de valójában két feladatot is ellát: biztonsági mentést készít és terheléselosztást végez. Amennyiben egy kiszolgáló meghibásodik vagy túlterheltté válik, egy másik veszi át a szerepét.

A farmot alkotó kiszolgálók állványba szerelhetők, a köztük fennálló összeköttetést pedig nagyon nagy sebességű (Gigabit Ethernet vagy gyorsabb) kapcsolók biztosítják. Amennyiben közös házba szerelt pengeszerverekről (blade server) van szó, a köztük fennálló összeköttetést a házon belüli nagysebességű hátlap (backplane) kapcsolat biztosítja.

A vállalati hálózati központ másik fontos feladata, hogy nagysebességű és nagy kapacitású adattárházként működjön. Az adattárház vagy hálózati adattároló (Network Attached Storage, (NAS) nagyszámú lemezmeghajtót foglal közvetlenül a hálózatra csatlakoztatott csoportba, bármely kiszolgáló számára elérhető módon. Egy NAS eszköz általában az Ethernetre kapcsolódik és saját IP címmel rendelkezik.

A tárolóhálózat (Storage Area Network, SAN) a hálózati adattárolók sokkal kifinomultabb változata. A tárolóhálózat olyan nagy sebességű hálózat, amely különböző típusú adattároló eszközöket kapcsol össze helyi vagy nagytávolságú hálózaton keresztül.

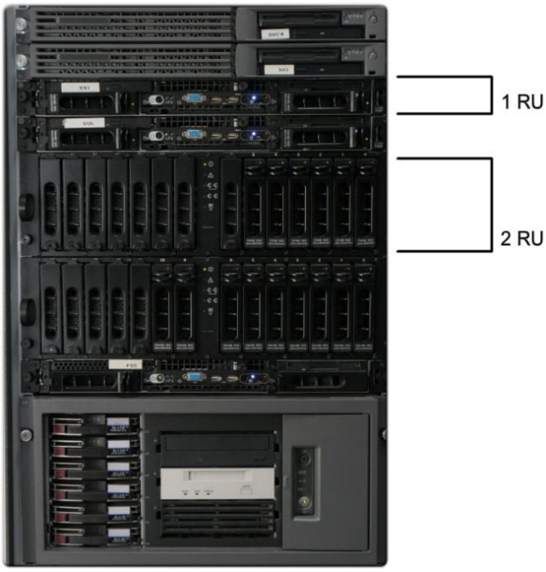

Kiszolgálófarm


Hálózati adattároló (NAS)

A vállalati hálózati központ berendezései általában állványba vannak szerelve. A nagyobb hálózati központokban az állványok a padlótól a mennyezetig érnek, és egymáshoz rögzítettek. A berendezések állványba szerelésekor ügyeljünk a megfelelő szellőzésre, valamint arra, hogy elölről és hátulról is hozzá lehessen férni az eszközökhöz! A berendezéseket megfelelő földeléshez is csatlakoztatni kell!

A legelterjedtebb állványok szélessége 48,26 cm (19 hüvelyk). A legtöbb berendezés mérete ehhez igazodik. A berendezések által függőlegesen elfoglalt teret tartókeret-egységben (Rack Unit, RU) adják meg. Egy ilyen egység 4,4 cm (1,75 hüvelyk). A 2U-val jelölt panel magassága például 8,9 cm (3,5 hüvelyk). Minél kisebb az RU szám, annál kevesebb helyet foglal el egy eszköz, így több eszköz férhet egy állványba.

Azt is figyelembe kell venni, ha egy berendezés sok összeköttetéssel rendelkezik (pl. egy kapcsoló)! Ezeket célszerű a kábelrendező panelek és a kábeltartó tálcák közelében elhelyezni.



Egy vállalat hálózati központjába kábelek ezrei futnak be, illetve onnan ki. Strukturált kábelezéssel olyan szervezett kábelrendszer alakítható ki, amely könnyen átlátható a telepítők, hálózati rendszergazdák és bármely más, a kábelekkel dolgozó szakemberek számára.

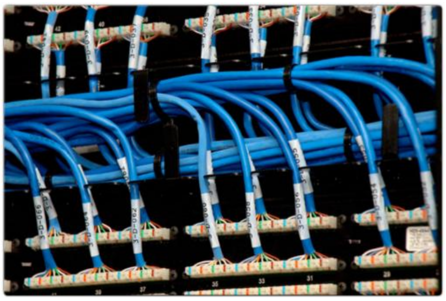
A kábelkezelés többféle célt szolgál. Egyrészről átlátható és szervezett rendszert eredményez, amely segít a kábelezési problémák izolálásában. Másrészről a megfelelő kábelezési módszerek biztosítják a kábelek védelmét a fizikai sérülésekkel és az elektromágneses zavarokkal (EMI) szemben, ami nagymértékben csökkenti a felmerülő problémák számát.

A hibaelhárítás megkönnyítéséhez az alábbi feladatokat célszerű elvégezni:

- Érdemes felcímkézni az összes kábel mindkét végét valamilyen – a forrást és a célt is jelölő – konvenció alapján.
- Érdemes feltüntetni az összes kábelnyomvonalat a fizikai hálózati topológia diagramon.
- Érdemes ellenőrizni az összes – mind a réz, mind az optikai – kábelnyomvonalat egyik végétől a másikig. Ehhez küldjünk végig egy vizsgálójelet a kábelen, majd mérjük meg a jelveszteséget!

A kábelszabványok az összes kábeltípushoz és hálózati technológiához meghatározzák az áthidalható maximális távolságot. Az IEEE például meghatározza, hogy az árnyékolatlan csavart érpáron (UTP) keresztüli Fast Ethernet technológia esetében a kapcsoló és az állomás közötti kábelnyomvonal hossza nem lehet több mint 100 méter (körülbelül 328 láb). Amennyiben a kábelnyomvonal hossza meghaladja a javasolt mértéket, adatátviteli problémák merülhetnek fel. Ez különösen igaz, ha a kábelvégződések rossz minőségűek.

A hálózat működtetéséhez nélkülözhetetlen a kábelezési és ellenőrzési terv megfelelő dokumentálása.



2.1.3 A telekommunikációs helyiség kialakításának szempontjai

A hálózati központ a vállalat központi idegrendszere. A gyakorlatban azonban a legtöbb felhasználó egy, a hálózati központtól távolabb eső telekommunikációs helyiség kapcsolójához csatlakozik. A telekommunikációs helyiséget huzalozási központnak vagy közbülső kábelrendezőnek (Intermediate Distribution Facility, IDF) is nevezik. A távközlési helyiségben a hozzáférési réteg hálózati eszközei vannak, és ideális esetben a hálózati központhoz hasonló körülményeket (pl. légkondicionálót és UPS-t) biztosít.

A vezetékes technológiát használó felhasználók Ethernet kapcsolón vagy hubon keresztül, a vezeték nélküli technológiát használó felhasználók pedig hozzáférési ponton (Access Point, AP) keresztül csatlakoznak a hálózathoz. A hozzáférési réteg eszközei (pl. a kapcsolók és a hozzáférési pontok) hálózatbiztonsági szempontból lehetséges veszélyforrások. Az ilyen berendezésekhez történő fizikai és távoli hozzáférést az arra illetékes személyekre kell korlátozni. A hálózati személyzet a kapcsolókon többek között portvédelmet, a hozzáférési pontokon pedig különféle vezeték nélküli biztonsági intézkedéseket alkalmazhat.

A telekommunikációs helyiség védelme még fontosabbá vált az ID (felhasználónév, jelszó) identitáslopások megnövekedett száma miatt. Az új, személyes adatok kezelését szabályozó törvények súlyosan büntetik, ha egy hálózatról bizalmas adatok kerülnek illetéktelen kezekbe. A korszerű hálózati eszközök funkciókínálata segít az ilyen típusú támadások megelőzésében, valamint az adat- és felhasználói integritás megőrzésében.

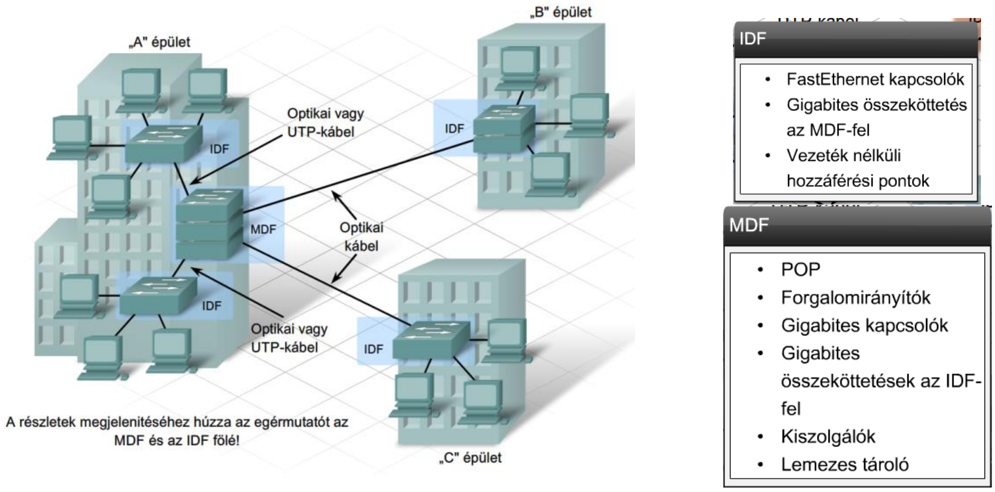


Egy központi kábelrendezőhöz (Main Distribution Facility, MDF) számos IDF csatlakozhat kiterjesztett csillag topológiának megfelelő elrendezésben. Az MDF általában a hálózati központban vagy az épület közepén helyezkedik el.

Az MDF általában lényegesen nagyobb, mint egy IDF. Az MDF-ben nagysebességű kapcsolók, forgalomirányítók és kiszolgálófarmok találhatók. A központi MDF kapcsolóihoz vállalati kiszolgálók és adattárolók is csatlakozhatnak, gigabites rézvezetéken keresztül.

Az IDF-ben alacsonyabb sebességű kapcsolók, hozzáférési pontok és hubok találhatók. Az IDF kapcsolói általában nagyszámú Fast Ethernet porttal rendelkeznek, hogy biztosítsák a felhasználók számára a hozzáférési rétegben történő csatakozást.

Az IDF kapcsolók általában gigabites interfészen keresztül csatlakoznak az MDF kapcsolókhoz. Ez az elrendezés hozza létre a gerinc- vagy más néven főkapcsolatokat (uplink). A réz alapú gigabites vagy Fast Ethernet összeköttetés hossza CAT5e vagy CAT6 kábel használatával legfeljebb 100 méter lehet. Optikai kábellel ennél lényegesen nagyobb távolság fedhető le. Optikai kábeleket általában az épületek közötti összeköttetéshez használnak. Mivel ezek nem villamos jeleket használnak, érzéketlenek a villámcsapásokkal, elektromágneses zavarral (EMI), rádiójel zavarral (RFI) és a különböző földpotenciálból adódó problémákkal szemben.

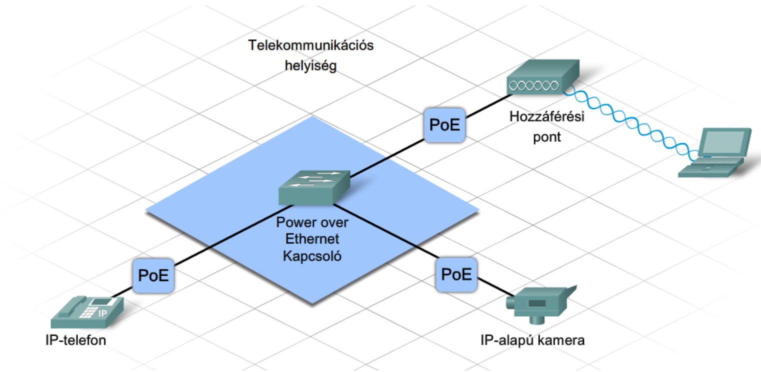


Az alapvető hálózati hozzáférésen kívül egyre elterjedtebb, hogy a végfelhasználói berendezések áramellátását is közvetlenül a telekommunikációs helyiségben található Ethernet kapcsolók biztosítják. Az ilyen tápellátást használó berendezések közé tartozik az IP-telefon, a hozzáférési pont és a megfigyelő kamera is.

A fenti eszközök áramellátása az Ethernet hálózat által biztosított áramellátást (Power over Ethernet, PoE) leíró, IEEE 802.3af szabvány alapján történik. A PoE ugyanazt a csavart érpáras kábelt használja az áramellátás biztosítására is, amin az adatátvitel történik. Így például lehetővé válik, hogy egy IP-telefon külön tápkábel vagy tápcsatlakozó nélkül kerüljön az asztalra. Az IP-telefonhoz hasonló PoE eszközök működtetéséhez a csatlakozást biztosító kapcsolónak PoE funkcióval kell rendelkeznie.

A PoE szabványt nem támogató kapcsolók alkalmazása esetén ún.áram-injektorok (power injectors) vagy PoE kábelrendezők használatával is megvalósítható az Ethernet hálózat által biztosított áramellátás. A Panduit és más gyártók készítenek olyan PoE kábelrendezőket, amelyek lehetővé teszik a PoE funkciókkal nem rendelkező kapcsolók számára a PoE környezetben történő működést. A

hagyományos kapcsolót a PoE kábelrendezőhöz kell csatlakoztatni, amely azután a PoE funkciókkal rendelkező eszközhöz kapcsolódik.



2.2 A vállalati perem támogatása

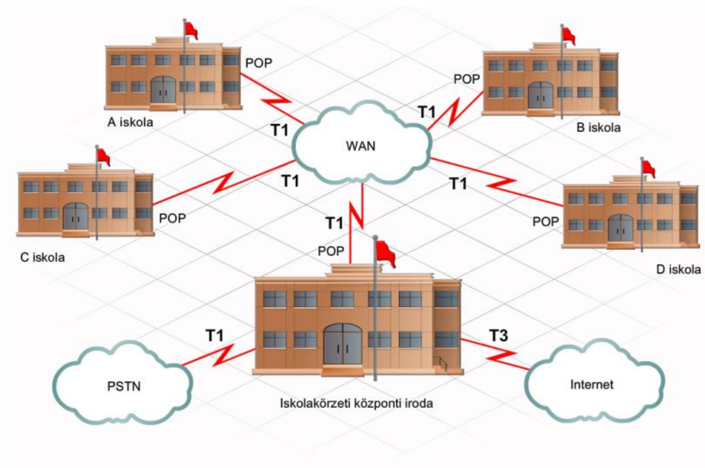
2.2.1 Szolgáltatás-átadás a szolgáltatás-elérési ponton

A vállalati hálózat külső határa a szolgáltatás-elérési pont (Point-of-Presence, POP), amely a vállalati hálózatba érkező szolgáltatások belépési pontja szolgál. A POP-on keresztül beérkező külső szolgáltatások közé tartoznak az internet-hozzáférés, a nagytávolságú kapcsolatok és a telefonszolgáltatás (PSTN).

A POP tartalmaz egy határpontot. A határpont kijelöli, hogy egy adott berendezése karbantartása és hibaelhárítása a szolgáltató (Service Provider, SP) vagy az ügyfél felelőssége. A szolgáltató által biztosított berendezésekért a határpontig a szolgáltató, azon túl pedig az ügyfél felel. A szolgáltató által biztosított berendezésekért a határpontig a szolgáltató, azon túl pedig mindenért az ügyfél felel.

A vállalatoknál a POP biztosítja a összeköttetést a külső szolgáltatások és telephelyek felé. A POP közvetlen összeköttetést biztosíthat egy vagy több internetszolgáltatóhoz, amely a belső felhasználók számára lehetővé teszi az igényelt internet-hozzáférést. A vállalatok távoli telephelyeit szintén a szolgáltatás-elérési pontokon keresztül kötik össze. Az ilyen telephelyek közötti nagytávolságú összeköttetést a szolgáltató hozza létre.

A POP és a határpont helye országonként eltérő lehet. Gyakran az ügyfél központi kábelrendezőjén belül kap helyet, de az internetszolgáltatónál is elhelyezkedhet.



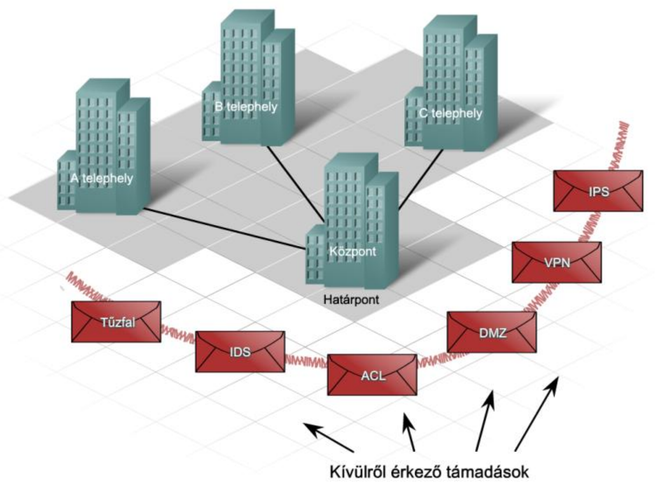
2.2.2 A vállalati határvonal biztonsági szempontjai

A nagyvállalatok általában több, egymással összeköttetésben lévő telephelyből állnak. Ezek mindegyike rendelkezhet olyan határkapcsolattal, amelyen keresztül a cég a külvilág egyéni felhasználóihoz és szervezeteihez kapcsolódik.

A határvonal a kívülről érkező támadások belépési pontja, és ez a pont rendkívül sebezhető. A határvonal ellen irányuló támadások felhasználók ezreit érinthetik. A szolgáltatásmegtagadásos (Denial of Service, DoS) támadások például megakadályozzák az erőforrásokhoz történő hozzáférést az arra jogosult felhasználók számára a hálózaton belül és kívül egyaránt, így csökkentik a vállalat termelékenységét.

A szervezet összes bejövő és kimenő forgalma keresztülhalad a határvonalon. A határvonal berendezéseit úgy kell konfigurálni, hogy védelmet nyújtsanak a támadások ellen, webhely, IP-cím, forgalmi minta, alkalmazás és a protokoll alapú szűrést biztosítsanak.

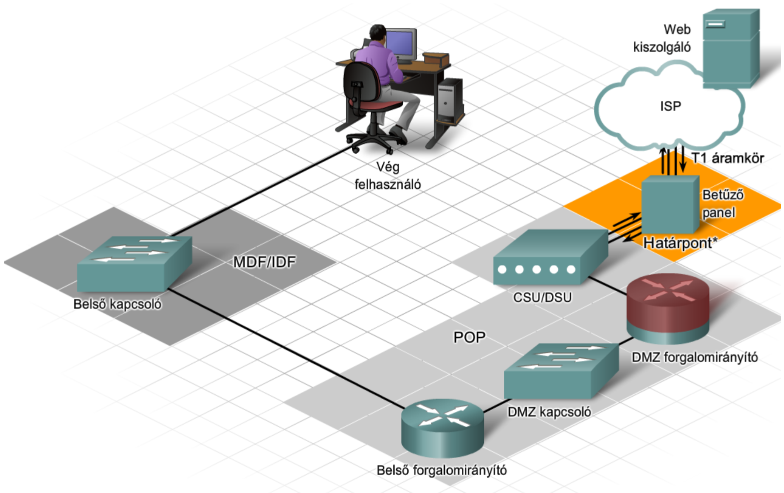
A hálózat védelméhez a szervezetek a határvonalnál tűzfalakat, valamint behatolás-érzékelő rendszerrel (Intrusion Detection System, IDS) és behatolás-megelőző rendszerrel (Intrusion Prevention System, IPS) felszerelt biztonsági eszközöket alkalmazhatnak.
A külső helyszínen dolgozó rendszergazdáknak a karbantartási feladatok és szoftvertelepítések elvégzéséhez hozzáférésre van szüksége a belső hálózathoz. Ez virtuális magánhálózatok (Virtual Private Network, VPN), hozzáférési listák (Access Control List, ACL), felhasználói azonosítók és jelszavak segítségével biztosítható. A VPN lehetővé teszi a belső erőforrásokhoz történő hozzáférést a távmunkát végzők számára is.



A vállalatok által megvásárolt hálózatkapcsolati szolgáltatások közé tartozik a bérelt vonal, a T1/E1 (más néven üzleti kategória), a Frame Relay és az ATM. A fenti szolgáltatások valamilyen fizikai kábelezésen keresztül jutnak el a vállalathoz. A T1/E1 általában rézvezetéket, a nagyobb sebességű szolgáltatások optikai kábelt használnak.

A szolgáltatás-elérési pontnak az aktuálisan igényelt WAN-szolgáltatáshoz szükséges összes berendezéssel rendelkeznie kell. A T1/E1 szolgáltatás esetében például az ügyfél igényelhet egy betűző panelt a T1/E1 áramkör végződtetéséhez, csakúgy mint egy csatornaszolgáltató / adatszolgáltató egységet (Channel Service Unit / Data Service Unit, CSU/DSU) a megfelelő elektromos interfész és a jelzésrendszer biztosításához a szolgáltató felé. A fenti berendezés tulajdonosa és

karbantartója a szolgáltató és az ügyfél egyaránt lehet. A tulajdonostól függetlenül minden, a szolgáltatás-elérési ponton belül, vagyis az ügyfél oldalán elhelyezett berendezést előfizetői végberendezésnek (Customer Premises Equipment, CPE) nevezünk.



*A határpont a szolgáltatóval kötött szolgáltatói szerződéstől függően eltérő lehet.

2.3 Az irányítás és a kapcsolás áttekintése

2.3.1 A forgalomirányító

A vállalati hálózat elosztási rétegének egyik fontos eszköze a forgalomirányító. Forgalomirányítás nélkül a csomagok nem lennének képesek elhagyni a helyi hálózatot.

A forgalomirányító hozzáférést biztosít más magánhálózatokhoz, valamint az internethez is. A forgalomirányító helyi interfészének IP-címét meg kell adni a helyi hálózat összes állomásának IP-beállításainál. A forgalomirányító ezen interfészét alapértelmezett átjárónak nevezzük.

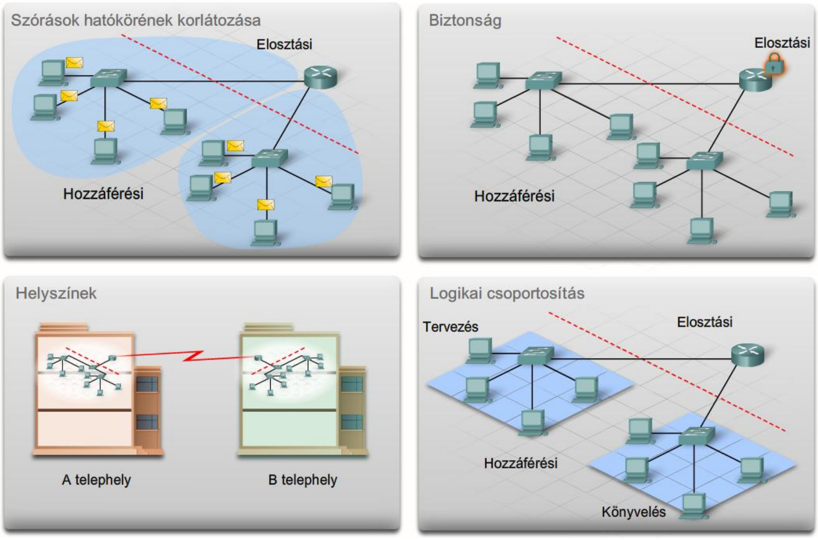
A forgalomirányítók szerepe a hálózatban kulcsfontosságú, mivel összeköttetést biztosítanak egy vállalati hálózat több telephelye között, redundáns útvonalakat kínálnak, és biztosítják az ISP-k közötti kapcsolatot az interneten keresztül. A forgalomirányítók betölthetik a tolmács szerepét is a különböző átviteli közegtípusok és protokollok között. A forgalomirányító például újracsomagolja az Ethernet hálózatból származó csomagokat a soros beágyazásnak megfelelően.

A forgalomirányító a cél IP-cím hálózati részét használja, hogy a csomagokat a megfelelő cél felé irányítsa. Ha megszűnik egy összeköttetés vagy torlódás alakul ki, akkor tartalékútvonalat jelöl ki.

A forgalomirányítók más hasznos funkciókat is ellátnak:

- A szórások kézben tartása
- Összeköttetés biztosítása távoli helyek között
- A felhasználók alkalmazási terület vagy szervezeti egység szerinti logikai csoportosítása
- Fejlett adatbiztonság megvalósítása (hálózati címfordítással és ACL-ekkel)

A vállalatok és az internetszolgáltatók számára egyaránt kulcsfontosságú a csomagok célba juttatásához a hatékony forgalomirányítás és a meghibásodott hálózati kapcsolatok helyreállítása.



Szórások hatókörének korlátozása

Az elosztási rétegben lévő forgalomirányítók a helyi hálózatra korlátozzák a szórásokat, ahol azokat hallani kell. Habár a szórásokra szükség van, az ugyanarra a helyi hálózatra csatlakoztatott túl sok állomás túlzott mértékű szórást generál, így lassítja a hálózat működését.

Biztonság

Az elosztási rétegben található forgalomirányítók elkülönítik és védik a bizalmas információt tároló számítógépek bizonyos csoportjait. A forgalomirányítók ezen felül a belső számítógépek címeit a külvilág elől elrejtve segítenek a támadások megakadályozásában, valamint szabályozzák, hogy ki érheti el vagy hagyhatja el a helyi hálózatot.

Helyszínek

Az elosztási rétegben található forgalomirányítók összeköttetést biztosíthatnak egy szervezet különböző (sokszor földrajzilag elkülönülő) telephelyeinek hálózatai között.

Logikai csoportosítás

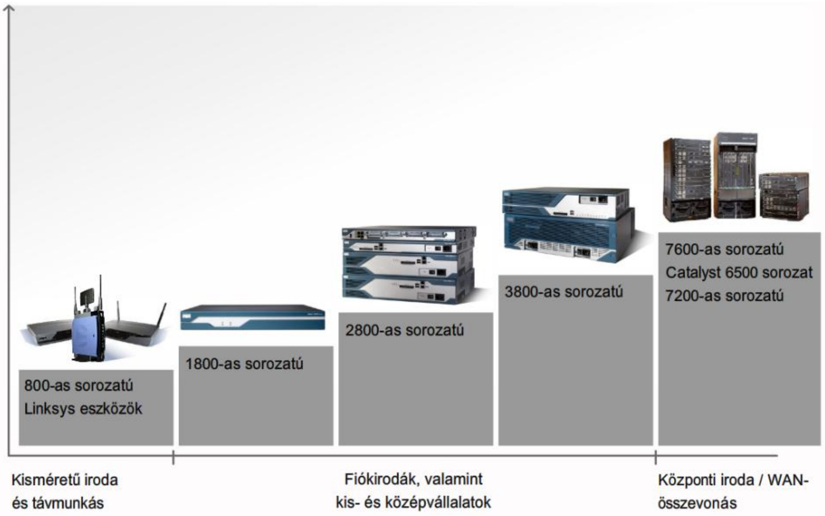
Az elosztási rétegben található forgalomirányítók logikailag csoportosítják a felhasználókat, például a vállalat hasonló igényekkel rendelkező vagy ugyanazokhoz az erőforrásokhoz hozzáférést igénylő osztályai alapján.

A forgalomirányítók többféle alakban és méretben kaphatók. Egy vállalati környezetben dolgozó hálózati rendszergazdának a legkülönfélébb forgalomirányítókhoz és kapcsolókhoz kell támogatást nyújtani, az asztalitól kezdve az állványba szerelhetőn át a penge modellekig.

A forgalomirányítók az alapján is csoportosíthatók, hogy a hardverkonfigurációjuk rögzített vagy moduláris. A rögzített konfiguráció esetében a forgalomirányító interfészei fixen beépítettek. A moduláris forgalomirányítókat több bővítőhellyel szállítják, amelyek lehetővé teszik a hálózati rendszergazdák számára a forgalomirányító interfészeinek cseréjét. A Cisco 1841-es forgalomirányítót például két beépített Fast Ethernet RJ-45 interfésszel szállítják, és van két – számos különböző típusú hálózati csatlakozómodul fogadására alkalmas – bővítőhelye is.

A forgalomirányítókat a legkülönfélébb (pl. Fast Ethernet, Gigabit Ethernet, soros, száloptikai) interfészekkel szállítják. A forgalomirányító interfészeinek megnevezése a vezérlő/interfész vagy a vezérlő/bővítőhely/interfész konvenciót követi. Ha például a vezérlő/interfész konvenciót használjuk, a forgalomirányítón az első Fast Ethernet interfészt az Fa0/0 (0. vezérlő és 0. interfész) jelöli. A

másodikat az Fa0/1. A vezérlő/bővítőhely/interfész konvenciót használó forgalomirányítón az első soros interfészt az S0/0/0 jelöli.



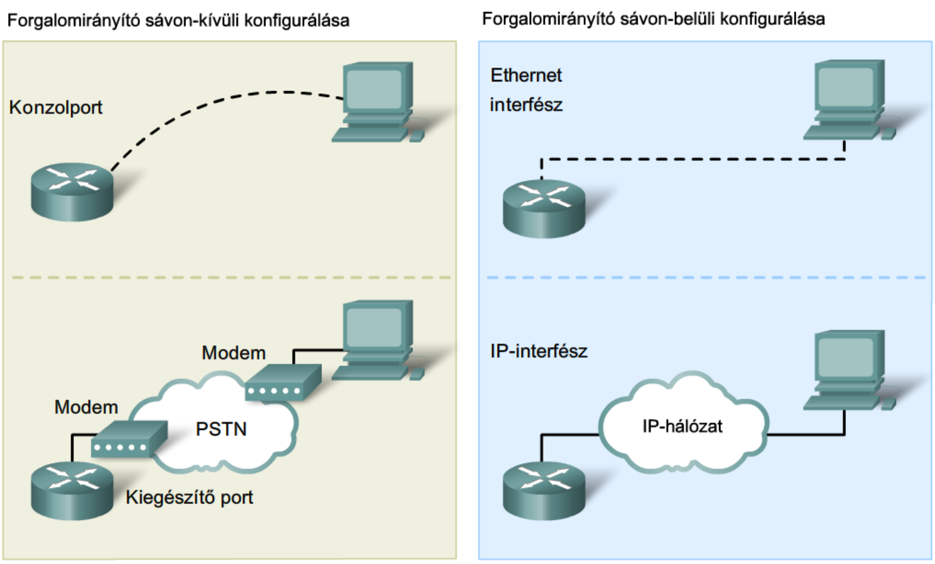
Két módszer létezik egy PC és egy hálózati eszköz konfigurációs és ellenőrzési feladatok céljából történő összekapcsolására: a sávon kívüli és a sávon belüli vezérlés.

A sávon kívüli vezérlés a kezdeti konfiguráció megadásához vagy hálózati kapcsolat hiánya esetén használható. A sávon kívüli vezérlést használó konfigurációhoz az alábbiak szükségesek:

- Közvetlen összeköttetés a konzol- vagy AUX-porttal
- Terminálemulációs ügyfélprogram

A sávon belüli vezérlés egy hálózati eszköz hálózati kapcsolaton keresztül történő ellenőrzésére és a konfigurációs beállítások elvégzésére használható. A sávon belüli vezérlést használó konfigurációhoz az alábbiak szükségesek:

- Legalább egy csatlakoztatott és működőképes hálózati interfész az eszközön
- Telnet, SSH vagy HTTP kapcsolaton keresztül elérhető Cisco eszköz



2.3.2 A forgalomirányító parancssoros felületének alapvető show parancsai

Az alábbiakban a forgalomirányító működési állapotának és hálózati funkcionalitásának megjelenítéséhez, illetve ellenőrzéséhez használható leggyakoribb IOS parancsok közül következik néhány. Az alábbi parancsok több kategóriába sorolhatók.

Általános használatú:

- `show running-config`
- `show startup-config`
- `show version`

Forgalomirányítással kapcsolatos:

- `show ip protocols`
- `show ip route`

Interfésszel kapcsolatos:

- `show interfaces`
- `show ip interface brief`
- `show protocols`

Összeköttetéssel kapcsolatos:

- `show cdp neighbors`
- `show sessions`
- `show ssh`
- `ping`
- `traceroute`

Teljes parancs	Rövidítés	Cél / Megjelenített információ
Általános célú parancsok		
`show running-config`	`sh run`	Megjeleníti a RAM-ból futó jelenlegi konfigurációt. Tartalmazza az állomásnevet, jelszavakat, az interfészek IP-címét, az aktivált irányító protokollt, a DHCP és a NAT beállításait. A parancs kiadása EXEC módban lehetséges.
`show startup-config`	`sh star`	Megjeleníti az NVRAM-ba elmentett tartalékkonfigurációt. Eltérő lehet, amennyiben az aktív konfigurációt nem mentették el. A parancs kiadása EXEC módban lehetséges.
`show version`	`sh ve`	Megjeleníti az IOS verziót, a ROM verziót, a forgalomirányító futási idejét, a rendszer képállományának nevét, a betöltési módot, az interfészek számát és típusát, a RAM, NVRAM és flash mennyiségét, valamint a konfigurációs regiszter értékét.
Forgalomirányítással kapcsolatos parancsok		
`show ip protocols`	`sh ip pro`	Megjeleníti a beállított forgalomirányító protokollok adatait, beleértve az időzítési beállításokat, verziószámokat, frissítési időközöket, az aktív interfészeket és a hirdetett hálózatokat.
`show ip route`	`sh ip ro`	Megjeleníti az irányítótábla adatait, beleértve az irányítási kódot, az ismert hálózatokat, azok adminisztratív távolságát és a metrikát, a megtanulásuk módját, a következő ugrás utolsó frissítését, az interfészt, amelyen keresztül a tanulás történt, és valamennyi beállított statikus útvonalat (beleértve az alapértelmezettet is).
Interfésszel kapcsolatos parancsok		
`show interfaces (type #)`	`sh int f0/0`	Megjeleníti egy vagy az összes interfész vonali (protokoll) állapotát, sávszélességét, megbízhatóságát, beágyazását, duplex és I/O statisztikáit.
`show ip interface brief`	`sh ip int br`	Megjeleníti az összes interfész IP-címét, interfész állapotát (up/down/admin down) és a vonali protokoll állapotát (up/down).
`show protocols`	`sh prot`	Megjeleníti az összes interfész IP-címét és alhálózati maszkját (/ jelöléssel), interfész állapotát (up/down/admin down) és a vonali protokoll állapotát (up/down).
Kapcsolatokra vonatkozó parancsok		
`show cdp neighbors (detail)`	`sh cdp ne`	Megjeleníti a közvetlenül csatlakoztatott eszközök adatait, beleértve az eszközazonosítót (állomásnév), az interfészt, amelyhez az eszköz csatlakoztatva van, a képességét (R=forgalomirányító, S=kapcsoló), a platformot (pl.: 2620XM) és a távoli eszköz portazonosítóját.A details opció ezen felül megadja a másik eszköz IP-címét, valamint IOS verzióját.
`show sessions`	`sh ses`	Megjeleníti a távoli állomásokkal létesített telnetkapcsolatokat (VTY). Megjeleníti a kapcsolatazonosítót, az állomásnevet és a címet.
`show ssh`	`sh ssh`	Megjeleníti a távoli állomásokkal létesített ssh kiszolgálói kapcsolatokat.
`ping (IP-cím / állomásnév)`	`P`	5 ICMP-visszhangkérést küld egy IP-címre vagy állomásnévre (amennyiben a DNS elérhető), majd megjeleníti a minimális/maximális és átlagos válaszidőt.
`traceroute (IP-cím / állomásnév)`	`Tr`	Változó élettartamú (TTL) visszhangkérést küld. Kilistázza az útba eső forgalomirányítókat (ugrások) és válaszidejüket.

2.3.3 A forgalomirányító alapbeállításainak megadása a parancssoros felületről

A forgalomirányító alapbeállításainak részét képezi az azonosítás céljából megadott állomásnév, a biztonsági célból megadott jelszavak beállítása, valamint az IP-címek interfészekhez történő hozzárendelése az összeköttetés biztosításához. Ellenőrizzük a konfigurációt, majd mentsük el a

változtatásokat a copy running-config startup-config parancs használatával! A forgalomirányító beállításainak törléséhez használjuk az erase startup-config, majd a reload parancsot!

Konfigurációkezelés:

- `enable`
- `configure terminal`
- `copy running-config startup-config`
- `erase startup-config`
- `reload`

Globális beállítások:

- `hostname`
- `banner motd`
- `enable password`
- `enable-secret`

Vonali beállítások:

- `line con`
- `line aux`
- `line vty`
- `login and password`

Interfészbeállítások:

- `interface típus/szám`
- `description`
- `ip address`
- `no shutdown`
- `clock rate`
- `beágyazás (encapsulation)`

Forgalomirányítási beállítások:

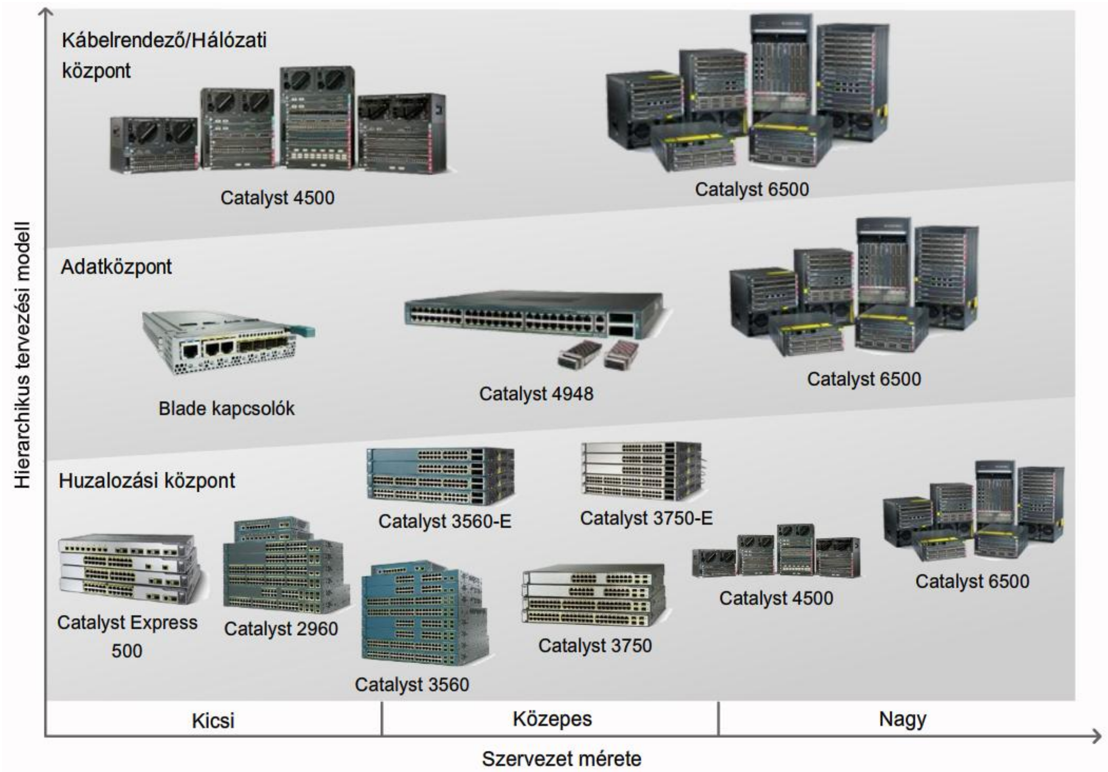
- `router`
- `network`
- `ip route`

2.3.4 A kapcsoló

A hierarchikus tervezési modell mindhárom rétege tartalmaz ugyan kapcsolókat és forgalomirányítókat, a hozzáférési rétegben általában több a kapcsoló. A kapcsolók fő feladata, hogy biztosítsák az állomások (pl. végfelhasználói munkaállomások, kiszolgálók, IP-telefonok, webkamerák, hozzáférési pontok és forgalomirányítók) közötti összeköttetést. Ez azt jelenti, hogy egy vállalatnál lényegesen több kapcsolóra van szükség, mint forgalomirányítóra.

A kapcsolók többféle formátumban kaphatók:

- Léteznek kisméretű, asztali vagy falra szerelhető modellek.
- Az állványba szerelhető, integrált forgalomirányítók részét képezi egy beépített kapcsoló.
- A nagyteljesítményű kapcsolók általában állványba szerelhetők, kialakításuk jellemzően moduláris a panel- és penge modellre épül, amely képes követni a felhasználók számának növekedését.

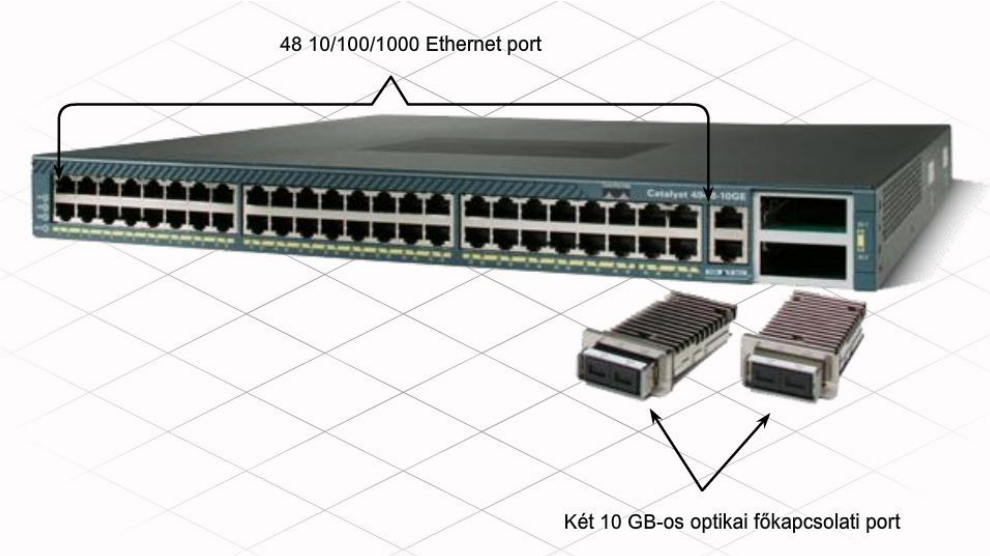


A nagyteljesítményű vállalati és szolgáltatói kapcsolók támogatják a 100 Mbit/sec-tól 10 Gbit/sec-ig terjedő, különböző sebességű portokat.

Egy vállalati MDF kapcsoló gigabites optikai vagy rézkábellel csatlakozik az IDF kapcsolókhoz. Az IDF kapcsolóknak általában mindkét RJ-45 Fast Ethernet portra szükségük van, de kell legalább egy gigabites Ethernet port is (réz vagy optikai) az MDF kapcsolóhoz történő felcsatlakozáshoz. A nagyteljesítményű kapcsolók némelyike moduláris portokkal rendelkezik, amelyek szükség esetén cserélhetők. Ilyen cserére lehet szükség például akkor, ha többmódusú optikai kábelről, eltérő típusú portot igénylő egymódusúra váltunk.

A forgalomirányítókhoz hasonlóan a kapcsolók portjait is a vezérlő/port vagy a vezérlő/bővítőhely/port konvenció alapján jelöljük. Ha például a vezérlő/port konvenciót használjuk, akkor a kapcsoló első Fast Ethernet portját az Fa0/1 (0. vezérlő, 1. port) jelöli. A másodikat az Fa0/2. A vezérlő/bővítőhely/port konvenciót használó kapcsoló első portja az Fa0/0/1. A gigabites portokat a Gi0/1, Gi0/2, stb. jelölik.

A kapcsolók portsűrűsége szintén lényeges szempont. Vállalati környezetben, ahol felhasználók százainak és ezreinek kell csatlakozni valamilyen kapcsolóhoz, egy 48 portos, 1RU magasságú kapcsoló portsűrűsége nagyobb, mint egy 24 portos, 1RU magasságú kapcsolóé.



2.3.5 A kapcsoló parancssoros felületének parancsai

A kapcsolón a beállítások megadása, az összeköttetés ellenőrzése és a kapcsoló jelenlegi állapotának megjelenítése IOS parancsok segítségével történik. Ezek a parancsok számos kategóriába sorolhatók az alábbiak szerint:

Általános használatú:

- `show running-config`
- `show startup-config`
- `show version`

Interfésszel / porttal kapcsolatos:

- `show interfaces`
- `show ip interface brief`
- `show port-security`
- `show mac-address-table`

Összeköttetéssel kapcsolatos:

- `show cdp neighbors`
- `show sessions`
- `show ssh`
- `ping`
- `traceroute`

A forgalomirányítóknál alkalmazott sávon belüli és sávon kívüli konfigurálási technikák a kapcsoló beállításánál is ugyanúgy használhatók.

Teljes parancs	Rövidítés	Cél / Megjelenített információ
Általános célú parancsok		
`show running-config`	`sh run`	Megjeleníti a RAM-ból futó jelenlegi konfigurációt. Tartalmazza az állomásnevet, jelszavakat, az interfészek IP-címét (amennyiben van ilyen), a portszámokat és a jellemzőket (duplex/sebesség).
`show startup-config`	`sh star`	Megjeleníti az NVRAM-ba elmentett tartalékkonfigurációt. Eltérő lehet, amennyiben az aktív konfigurációt nem mentették el.
`show version`	`sh ve`	Megjeleníti az IOS verziót, a ROM verziót, a kapcsoló futási idejét, a rendszer képállományának nevét, a betöltési módot, az interfészek számát és típusát, a RAM, NVRAM és flash mennyiségét, valamint a konfigurációs regiszter értékét.
Interfésszel / porttal kapcsolatos parancsok		
`show interfaces (type #)`	`sh int f0/1`	Megjeleníti egy vagy az összes interfész vonali (protokoll) állapotát, sávszélességét, megbízhatóságát, beágyazását, duplex és I/O statisztikáit.
`show ip interface brief`	`sh ip int br`	Megjeleníti az összes interfészt az IP-címmel, interfész állapottal (up/down/admin down) és a vonali protokoll állapotát (up/down).
`show port-security`	`sh por`	Megjeleníti az összes olyan portot, amelyen aktiválták a védelmet, ideértve a címek maximális számát, a jelenlegi számlálót, a behatolásérzékelő számlálót és a tervezett lépést (normál esetben a port lekapcsolása).
`show mac-address-table`	`sh mac-a`	Megjeleníti a kapcsoló által megtanult összes MAC-címet, megtanulásuk módját (dinamikus/statikus), a hozzá tartozó portszámot, valamint azt, hogy melyik VLAN-ba tartozik.
Kapcsolatokra vonatkozó parancsok		
`show cdp neighbors (detail)`	`sh cdp ne`	Megjeleníti a közvetlenül csatlakoztatott eszközök adatait, beleértve az eszközazonosítót (állomásnév), az interfészt, amelyhez az eszköz csatlakoztatva van, a képességét (R=forgalomirányító, S=kapcsoló), a platformot (pl.: WS-2950-2) és a távoli eszköz portazonosítóját. A details opció ezen felül megadja a másik eszköz IP-címét, valamint IOS verzióját.
`show sessions`	`sh ses`	Megjeleníti a távoli állomásokkal létesített telnetkapcsolatokat (VTY). Megjeleníti a kapcsolatazonosítót, az állomásnevet és a címet.
`show ssh`	`sh ssh`	Megjeleníti a távoli állomásokkal létesített ssh kiszolgálói kapcsolatokat.
`ping (IP-cím / állomásnév)`	`p`	5 ICMP-visszhangkérést küld egy IP-címre vagy állomásnévre (amennyiben a DNS elérhető), majd megjeleníti a minimális/maximális és átlagos válaszidőt.
`traceroute (IP-cím / állomásnév)`	`tr`	Változó élettartamú (TTL) visszhangkérést küld. Kilistázza az útba eső forgalomirányítókat (ugrások) és válaszidejüket.

A kapcsoló alapbeállításainak részét képezi az azonosítás céljából megadott állomásnév, a biztonsági célból megadott jelszavak, valamint az IP-címek interfészekhez történő hozzárendelése az összeköttetés biztosításához. A sávon belüli hozzáféréshez a kapcsolónak IP-címmel kell rendelkeznie.

Ellenőrizzük, majd mentsük el a kapcsoló konfigurációját a copy running-config startup-config parancs használatával! A kapcsoló beállításainak törléséhez használjuk az erase startup-config, majd a reload parancsot! Szükség lehet a VLAN információk törlésére is, amely a delete flash:vlan.dat paranccsal végezhető el.

Konfigurációkezelés:

- `enable`
- `configure terminal`
- `copy running-config startup-config`
- `erase startup-config`
- `delete flash:vlan.dat`
- `reload`

Globális beállítások:

- `hostname`
- `banner motd`
- `enable password`
- `enable-secret`
- `ip default-gateway`

Vonali beállítások:

- `line con`
- `line vty`
- `login and password`

Interfészbeállítások:

- `interface type/number (vlan1)`
- `ip address`
- `speed / duplex`
- `switchport port-security`

2.4 A fejezet összefoglalása

- A hálózatszerkezeti diagram dokumentálja a hálózat eszközeit.
- A hálózati dokumentáció részét képezi az üzletfolytonossági terv, az üzletbiztonsági terv, a hálózat-karbantartási terv, valamint a szolgáltatási szerződések.
- A hálózati központ kezeli és felügyeli az összes hálózati erőforrást.
- A végfelhasználók az IDF-ben található hozzáférési rétegbe tartozó kapcsolón és vezeték nélküli hozzáférési ponton (Access Point, AP) keresztül csatlakoznak a hálózathoz.
- A PoE az adatátviterlre ugyanazt a csavart érpáras kábelt használja az áramellátás biztosítására.
- A vállalati határ biztosítja a szervezeten belüli felhasználók számára az internet-hozzáférést és -szolgáltatást.
- A POP közvetlen összeköttetést biztosít az internetszolgáltató felé, és kapcsolatot biztosít a távoli telephelyek között.
- A POP tartalmaz egy határpontot, amely kijelöli, hogy meddig tart a szolgáltató és az ügyfél felelőssége.
- A határeszközök biztosítják a támadások elleni védelmet.
- A szolgáltatások rézvezetéken vagy optikai kábelen keresztül jutnak el a vállalkozáshoz.
- A hozzáférési rétegbe tartozó kapcsolók biztosítják a hálózati összeköttetést a végfelhasználók számára.
- Az elosztási rétegbe tartozó forgalomirányítók mozgatják a csomagokat a különböző helyek és az internet között.
- A forgalomirányító és a kapcsoló sávon belüli és sávon kívüli vezérlést használ.
- A forgalomirányító képes a szórások korlátozására.

3. Kapcsolás vállalati hálózatokban

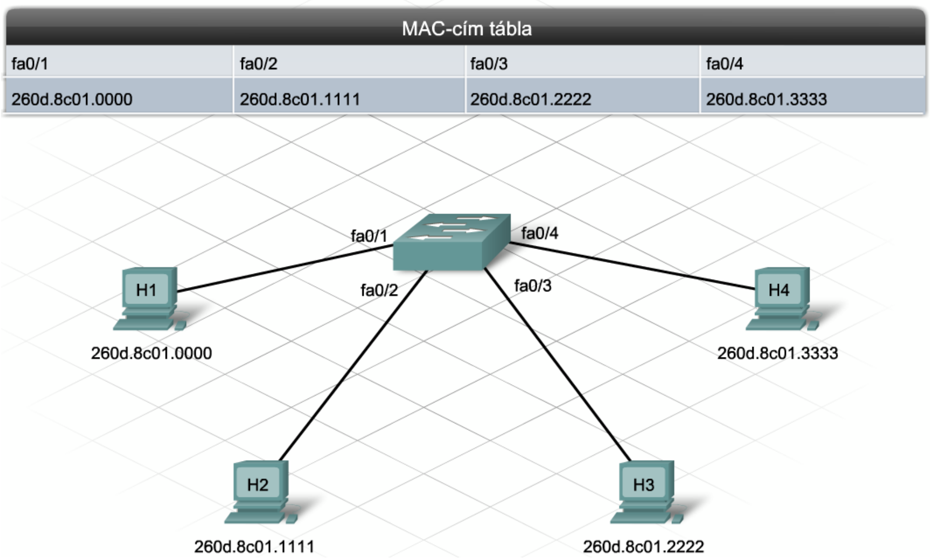
3.1 A vállalati szintű kapcsolási folyamatok megismerése

3.1.1 Kapcsolás és a hálózat szegmentálása

Azzal együtt, hogy a kapcsolók és a forgalomirányítók egyaránt részét képezik egy vállalati hálózatnak, a hálózat tervezése jelentős mértékben a kapcsolókon alapul. A kapcsolók portonkénti ára alacsonyabb, mint a forgalomirányítóké, és a keretek vezeték sebességű gyorstovábbítására képesek.

A kapcsoló egy nagyon jól alkalmazható 2. rétegbeli eszköz. Legegyszerűbb szerepében több állomás központi csatlakozópontjaként a hub-ot helyettesíti. A kapcsoló összetettebb szerepet is kaphat, ha egy vagy több másik kapcsolóhoz csatlakozik: redundáns kapcsolatokat és virtuális LAN (VLAN)-okat hozhat létre, kezelhet és tarthat karban. Egy kapcsoló minden típusú hálózati forgalmat egyformán kezel, függetlenül annak felhasználási módjától.

Egy kapcsoló a forgalmat a MAC-címek alapján továbbítja. Minden kapcsoló tartalmaz egy MAC-cím táblát, melyet tartalom szerint címezhető memóriának (content addressable memory, CAM) nevezett gyors hozzáférésű memóriában tárol. Minden egyes keret fogadásakor a memória tartalma frissül a forrás MAC-címe és a beérkezési port alapján.



Azzal együtt, hogy a kapcsolók és a forgalomirányítók egyaránt részét képezik egy vállalati hálózatnak, a hálózat tervezése jelentős mértékben a kapcsolókon alapul. A kapcsolók portonkénti ára alacsonyabb, mint a forgalomirányítóké, és a keretek vezeték sebességű gyorstovábbítására képesek.

A kapcsoló egy nagyon jól alkalmazható 2. rétegbeli eszköz. Legegyszerűbb szerepében több állomás központi csatlakozópontjaként a hub-ot helyettesíti. A kapcsoló összetettebb szerepet is kaphat, ha egy vagy több másik kapcsolóhoz csatlakozik: redundáns kapcsolatokat és virtuális LAN (VLAN)-okat

hozhat létre, kezelhet és tarthat karban. Egy kapcsoló minden típusú hálózati forgalmat egyformán kezel, függetlenül annak felhasználási módjától.

Egy kapcsoló a forgalmat a MAC-címek alapján továbbítja. Minden kapcsoló tartalmaz egy MAC-cím táblát, melyet tartalom szerint címezhető memóriának (content addressable memory, CAM) nevezett gyors hozzáférésű memóriában tárol. Minden egyes keret fogadásakor a memória tartalma frissül a forrás MAC-címe és a beérkezési port alapján.

Egy vállalatnál a nagymértékű rendelkezésre állás, a sebesség és a hálózat átbocsájtó képessége kritikus paraméterek. Az ütközési- és a szórási tartományok mérete erősen befolyásolja a hálózati forgalmat. Általában is elmondható, hogy a nagyobb ütközési- és szórási tartományok hatással vannak az említett létfontosságú paraméterekre.

Ha egy kapcsoló szórásos keretet kap, akkor az ismeretlen célcímű keret mintájára minden aktív interfészén kiküldi. A szórási tartományt azon eszközök csoportja alkotja, amelyek mind megkapják a szórásos keretet. Több kapcsoló összekapcsolásával a szórási tartományok mérete növekszik.

Az ütközési tartományok hasonló problémát okoznak. Minél több eszköz tartozik egy ütközési tartományhoz, annál több ütközés történik.

A hubok nagyméretű ütközési tartományokat hoznak létre. A kapcsolók ezzel szemben az úgynevezett mikroszegmentációval mindössze egyetlen kapcsolóportra csökkentik az ütközési tartományok méretét.

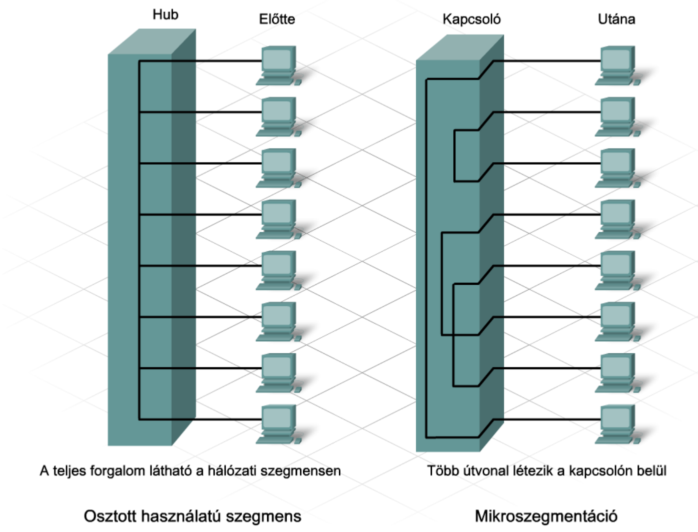
Ha a kapcsoló egy portjára csak egy állomás csatlakozik, akkor dedikált kapcsolat jön létre. Ha két csatlakozó állomás kommunikál egymással, akkor a kapcsolótábla alapján a kapcsoló egy virtuális kapcsolatot, más néven mikroszegmenst hoz létre a portok között.

A kapcsoló a keretátvitel végéig fenntartja a virtuális áramkört (VC). Több virtuális áramkör is lehet aktív egyszerre. A mikroszegmentáció az ütközések számának csökkentésével és több egyidejű kapcsolat fenntartásával javítja a sávszélesség kihasználását.

A kapcsolók szimmetrikus és aszimmetrikus kapcsolást is támogathatnak. Azok a kapcsolók, melyeknek minden portjuk azonos sebességű, szimmetrikus kapcsolást végeznek. Sok kapcsoló rendelkezik két vagy több nagysebességű porttal. Ezek a nagysebességű, más néven főkapcsolati (uplink) portok olyan nagy sávszélesség igényű kapcsolatokat hoznak létre, mint az alábbiak:

- Csatlakozás más kapcsolókhoz
- Összeköttetés kiszolgálókhoz és kiszolgálófarmokho
- Csatlakozás más hálózatokhoz

Különböző sebességű portok közötti adatátvitel esetén aszimmetrikus kapcsolásról beszélünk. Szükség esetén a kapcsoló eltárolja az információt a memóriában, s ezzel egy átmeneti tárolót biztosít a különböző sebességű portok között. Aszimmetrikus kapcsolók gyakran előfordulnak vállalati környezetben.



3.1.2 Többrétegű kapcsolás

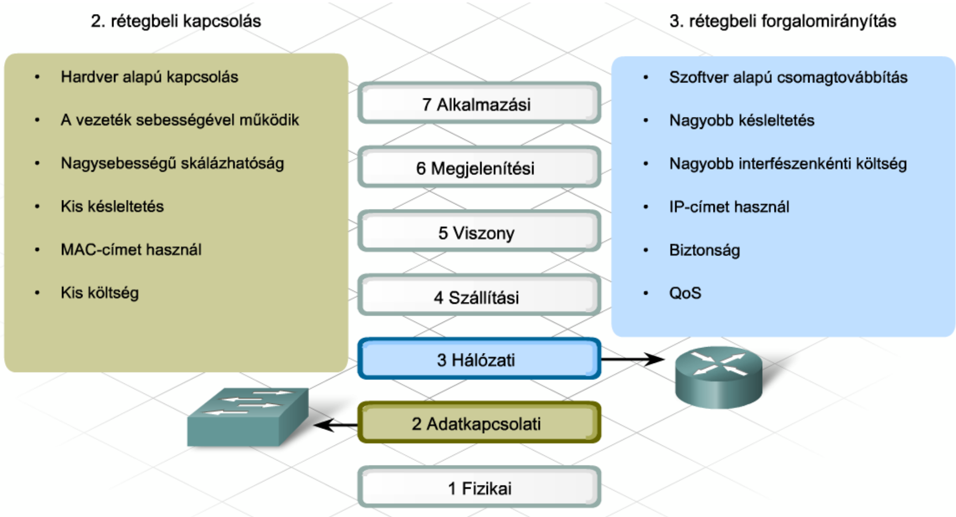
Hagyományosan a hálózatokat külön 2. és külön 3. rétegbeli eszközök alkották. Minden eszköz különböző technológiát használ az adatok feldolgozására és továbbítására.

2. réteg

2. rétegű kapcsolók hardver alapúak. Az adatforgalmat a bármely bejövő portot az összes többi porttal összekötő belső áramkörökkel, a vezeték sebességével továbbítják. A továbbítás a keretben és a MAC-táblában megtalálható cél MAC-cím alapján történik. Egy 2. rétegű eszköz az adatforgalmat csak egy hálózati szegmensen, alhálózaton belül továbbítja.

3. réteg

A forgalomirányítók szoftver alapúak, melyek mikroprocesszorok segítségével, IP-címek alapján hajtják végre a forgalomirányítást. A 3. rétegű forgalomirányítás lehetővé teszi az adatok továbbítását különböző hálózatok és alhálózatok között. Egy csomag beérkezésekor a forgalomirányító a szoftvere segítségével keresi meg a célállomás IP-címét és a célhálózat felé vezető legjobb útvonalat. A forgalomirányító ezek után a megfelelő interfészre kapcsolja a csomagot.



A 3. rétegű, vagy más néven többrétegű kapcsolás (multilayer switching) egyetlen eszközben egyesíti a hardver-alapú kapcsolást és a hardver-alapú forgalomirányítást.

Egy többrétegű kapcsoló egy 2. rétegbeli kapcsoló és egy 3. rétegbeli forgalomirányító tulajdonságait ötvözi. A 3. rétegű kapcsolást külön erre a célra kifejlesztett, alkalmazás-specifikus integrált áramkörök (application-specific integrated circuit, ASIC) végzik. A keret- és csomagtovábbítás ugyanazon áramkörök segítségével történik.

A többrétegű kapcsolók gyakran elmentik vagy gyorsítótárba helyezik egy adatfolyam első csomagjának irányítási információit. Ez lehetővé teszi, hogy az adatfolyam többi csomagjánál már ne legyen szükség a keresési folyamatra, hiszen a szükséges információ a memóriában már megtalálható. Ez a gyorsítótáras megoldás is hozzájárul az ilyen eszközök nagy teljesítőképességéhez.



Cisco 2960-as Kapcsoló
2. réteg

Cisco 3560-as Kapcsoló
3. réteg

3.1.3 Kapcsolási módszerek

A kapcsolás bevezetésekor a kapcsolók csak az egyik eljárást támogatták a keretek egyik portról egy másik portra történő átkapcsolására alkalmazható két fő módszer közül. A két módszer a tárol-és-továbbít, illetve a közvetlen továbbítás. Mindkét módszernek léteznek előnyei és hátrányai.

Tárol-és-továbbít

Ennél a kapcsolási módnál a kapcsolás az egész keretet beolvassa és eltárolja a memóriában, mielőtt kiküldené a céleszköz felé. A ciklikus redundancia ellenőrző érték (cyclic redundancy check, CRC) kiszámításával ellenőrzi az adatbitek érvényességét. Ha a kiszámított érték egyezik a CRC mező tartalmával, akkor a kapcsoló továbbítja a keretet a célállomás felé. Ha a CRC értékek nem egyeznek, akkor a kapcsoló nem továbbítja a keretet. A CRC mező az Ethernet keret keretellenőrző (frame check sequence, FCS) mezőjében található.

Bár ez a módszer ugyan megakadályozza a hibás keretek továbbítását, nagy hátránya, hogy a lehető legnagyobb késleltetéssel jár. Ennek következtében ezt a kapcsolási módot leginkább olyan környezetben használják, ahol igen gyakoriak például az elektromágneses interferencia (EMI) okozta átvitelhibák.

Közvetlen kapcsolás

A másik gyakori kapcsolási módszer a közvetlen kapcsolás. Ennek a módszernek további két alváltozata létezik: a gyorstovábbítás és a töredékmentes kapcsolás. Mindkét esetben a kapcsoló a

teljes keret megérkezése előtt már elkezdi a keret továbbítását. w Mivel ebben az esetben a kapcsoló nem számítja ki és nem ellenőrzi a CRC értéket, sérült keretek is továbbításra kerülhetnek.

A gyorstovábbítás a kapcsolás leggyorsabb módja. A kapcsoló amint elolvassa a cél MAC-címet, azonnal elkezdi a keret továbbítását a megfelelő célportra. Ennek a módszernek a legkisebb a késleltetése, de ütközéstöredékeket és sérült kereteket egyaránt továbbít. Egy stabil, kis hibaarányú hálózatban ez a legmegfelelőbb kapcsolási módszer.

A töredékmentes kapcsolásnál a kapcsoló a továbbítás előtt megvárja a keret első 64 bájtját, majd átkapcsolja a keretet a célportra. A legrövidebb érvényes Ethernet keret ugyanis 64 bájt hosszú. Kisebb keretek általában ütközések következtében jönnek létre és ezeket ütközéstöredéknek (runt) hívjuk. A fentiek miatt az első 64 bájt ellenőrzésével elérhető, hogy a kapcsoló ütközéstöredékeket ne továbbítson.

A tárol-és-továbbít módszer jár a legnagyobb és a gyorstovábbítás a legkisebb késleltetéssel. A töredékmentes kapcsolás késleltetése az előző két érték között helyezkedik el. A töredékmentes kapcsolás a legmegfelelőbb választás olyan környezetben, ahol sok az ütközés. A jól megtervezett hálózatoknál azonban az ütközés nem jelent problémát, így ilyen hálózatokban a gyorstovábbítás a legjobb módszer.

Manapság a legtöbb Cisco LAN kapcsoló a tárol-és-továbbít kapcsolási módszert alkalmazza, mivel az újabb technológiának és a gyorsabb feldolgozási időnek köszönhetően a kapcsolók hibázás nélkül képesek a közvetlen kapcsolással közel megegyező sebességgel az adatokat eltárolni és feldolgozni. Ezen felül a professzionális, például a többrétegű kapcsolók esetében mindenképpen a tárol-és-továbbít módszer kell alkalmazni.

Léteznek olyan újabb 2. és 3. rétegbeli kapcsolók, melyek képesek a változó hálózati körülményekhez alkalmazkodni.

Ezek a kapcsolók kezdetben a gyorstovábbítást alkalmazzák az elérhető legkisebb késleltetés érdekében. Ugyan a kapcsoló nem ellenőrzi a keretet a továbbítása előtt, de felismeri a hibákat, és a memóriában egy számláló segítségével nyilvántartja azok számát. A számláló értékét a kapcsoló időről-időre összeveti egy előre definiált küszöbértékkel.

Ha a hibák száma meghaladja a küszöbértéket, akkor ez a kapcsoló számára azt jelenti, hogy a továbbított hibás keretek mennyisége már nem elfogadható mértékű. Ebben az esetben a kapcsoló átvált tárol-és-továbbít kapcsolási módra. Ha a hibák száma visszaesik a küszöbérték alá, akkor a kapcsoló visszavált gyorstovábbításra. Ezt a módszert adaptív közvetlen kapcsolásnak hívjuk.



3.1.4 Kapcsolók védelme

Az alkalmazott kapcsolási módszertől függetlenül érdemes a hálózatunk védelméről gondoskodni. A hálózati biztonság témakörei leginkább a forgalomirányítókkal és a külső adatforgalom letiltásával foglalkoznak. A kapcsolókat általában a szervezeten belül használják, tervezésüknél az egyszerű kapcsolódási lehetőség biztosítása volt a cél, így nem vagy csak kevés biztonsági beállítás lehetséges rajtuk.

Az alábbi, kapcsolókon alkalmazható alapszintű biztonsági eljárások lehetővé teszik, hogy csak jogosult felhasználók férhessenek hozzá az eszközökhöz:

- Az eszköz fizikai védelme
- Titkosított jelszavak használata
- SSH elérés engedélyezése
- A hozzáférés és az adatforgalom felügyelete
- A http hozzáférés letiltása
- Nem használt portok letiltása
- A portvédelem engedélyezése
- A telnet letiltása

Titkos jelszavak

Minden jelszó (felhasználói mód, privilegizált mód és vty hozzáférés) legalább 6 nem ismétlődő karaktert tartalmazzon. Rendszeresen változtassa meg a jelszavakat! Sose használjon szótárban megtalálható szavakat! Használja az enable secret parancsot a privilegizált szintű hozzáférés védelmére, mivel ez fejlett titkosítási technikákat alkalmaz! Minden, az aktív konfigurációs fájlban megjelenő jelszót titkosítson a `service password-encryption` IOS paranccsal!

Fizikai biztonság

A kapcsolók kritikus összeköttetései a hálózatnak. Biztosítsa a kapcsolókat fizikailag egy rack-szekrényben rögzítve és a szekrény biztonságos helyen történő tárolásával! Korlátozza az eszközökhöz való hozzáférést csak az arra jogosult hálózati szakemberekre!

Az SSH engedélyezése a biztonságos távoli vty hozzáféréshez

Az SSH egy hálózaton keresztüli, másik eszközre történő belépést biztosító ügyfél-kiszolgáló alapú protokoll. Erős hitelesítést és biztonságos kommunikációt nyújt nem biztonságos csatornákon. Az SSH az egész belépési folyamatot titkosítja, beleértve a jelszavak átvitelét is.

A hozzáférés és forgalom felügyelete

Felügyelje a kapcsolón áthaladó forgalmat, annak garantálására, hogy a forgalom megfeleljen a vállalati irányelveknek! Ezen felül, jegyezze fel egy adott kapcsolóporthoz csatlakozó eszközök MAC-címét és a kapcsolóba történő bejelentkezési kísérleteket! Ha a kapcsoló rosszindulatú forgalmat vagy jogosulatlan hozzáférést észlel, tegyen intézkedéseket a szervezet biztonsági irányelveinek megfelelően!

A http hozzáférés letiltása

Tiltsa le a http hozzáférést a kapcsolóba történő weben keresztüli belépés és konfigurálás megakadályozása érdekében! A http hozzáférés letiltására használható a `no ip http server` parancs.

A nem használt portok letiltása

Tiltson le a kapcsolón minden nem használt portot az ismeretlen állomások vagy vezeték nélküli hozzáférési pontok kapcsolódásának megakadályozására! Ezt az interfészen kiadott `shutdown` paranccsal hajthatja végre.

Portbiztonság engedélyezése

A portbiztonság a kapcsoló egy megadott portján egy meghatározott MAC-cím listára korlátozza a hozzáférést. A MAC-címeket megadhatja manuálisan, vagy a kapcsoló dinamikusan is megtanulhatja azokat. A meghatározott kapcsoló port csak a megadott MAC-című eszközökről érkező forgalmat engedi át. Ha egy ettől eltérő MAC-című eszköz kapcsolódik a porthoz, akkor a kapcsoló automatikusan letiltja azt a portot.

Telnet letiltása

A telnet kapcsolatok segítségével nyilvános hálózaton keresztül küldhetünk adatokat, titkosítatlan formában. Ide tartoznak a felhasználói nevek, jelszavak és az adatok. Úgy tilthatja le minden hálózati eszköz telnettel történő elérését, hogy azokon egyik vty vonalon sem állít be belépési jelszót.

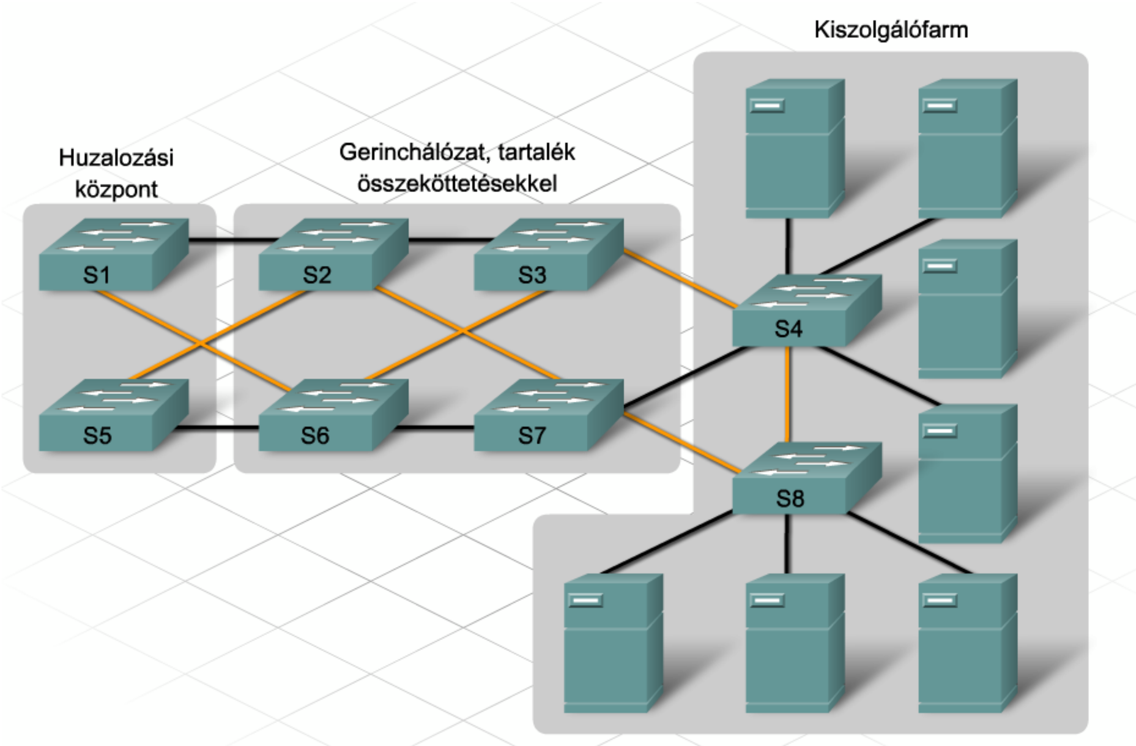
3.2 A kapcsolási hurkok kialakulásának megelőzése

3.2.1 Redundancia a kapcsolt hálózatokban

A modern vállalatok működőképessége egyre nagyobb mértékben függ a számítógépes hálózatuktól. Sok szervezet életképességét a hálózata határozza meg. A hálózat működésképtelensége komoly üzleti károkat, bevétel kiesést és az üzletfelek elégedetlenségét eredményezheti.

Egy összeköttetés, egy eszköz vagy egy kapcsoló kritikus portjának meghibásodása a hálózat működésképtelenségét okozza. A hálózat megtervezésekor redundanciára van szükség a magas szintű megbízhatóság fenntartása, valamint a meghibásodásra érzékeny és kritikus pontok csökkentése érdekében. A redundanciát a hálózati eszközök és a kritikus területek felé vezető összeköttetések duplázásával lehet megvalósítani.

Természetesen adódhatnak olyan helyzetek, amikor az összes összeköttetés és eszköz megduplázása nagyon költséges lenne. A hálózati mérnököknek általában mérlegelniük kell és egyensúlyt kell találni a redundanciával járó költségek és a hálózat rendelkezésre állási követelménye között.



A redundancia tulajdonképpen azt jelenti, hogy például egy adott cél felé két útvonal is létezik. Nem hálózati környezetben a redundanciára példaként az egy városba vezető két út, az egy folyót áthidaló két híd, vagy az egy épületből kivezető két ajtó esetét említhetjük. Ha az egyik út valamiért használhatatlan, a másik még elérhető.

A kapcsolók esetében redundanciát a köztük kialakitott többszörös összeköttetéssel érhetünk el. A kapcsolt hálózatokban megvalósított redundancia csökkenti a torlódásokat, bizosítja a nagymértékű rendelkezésre állást, valamint a terheléselosztást.

A kapcsolók között létrehozott összekötések ugyanakkor problémák forrásai is lehetnek. Az Ethernet forgalom szórásos jellege miatt például kapcsolási hurkok jöhetnek létre. A szórásos keretek körbe-körbe járnak minden irányban, szórási viharokat eredményezve. A szórási viharok az elérhető sávszélességet lefoglalják, így előfordulhat, hogy újabb hálózati kapcsolatok létrejöttét akadályozzák meg, valamint régiek megszakítását eredményezik.

Kapcsolt hálózatokban a szórási viharok mellett az egyedi címzésű keretek is okozhatnak problémát. Ilyen problématípus például a többszörös kerettovábbítás vagy a MAC-adatbázis instabilitása.

Többszörös kerettovábbítás

Ha egy állomás egyedi címzésű keretet küld egy olyan állomásnak, melynek MAC-címe egyetlenegy csatlakozó kapcsoló MAC-táblájában sem található meg, akkor mindegyik kapcsoló az összes portján kiküldi a keretet. Nem hurokmentes hálózatban a keret visszaérkezhet a kezdeményező kapcsolóhoz. A folyamat így újra meg újra megismétlődik, a keret többszörös példányát létrehozva a hálózaton.

Esetenként a célállomás több másolatot is kap az eredeti keretből. Ez három problémát is okozhat: sávszélesség felesleges lefoglalása, CPU időveszteség, valamint az adatforgalom esetleges duplázása.

MAC-adatbázis instabilitás

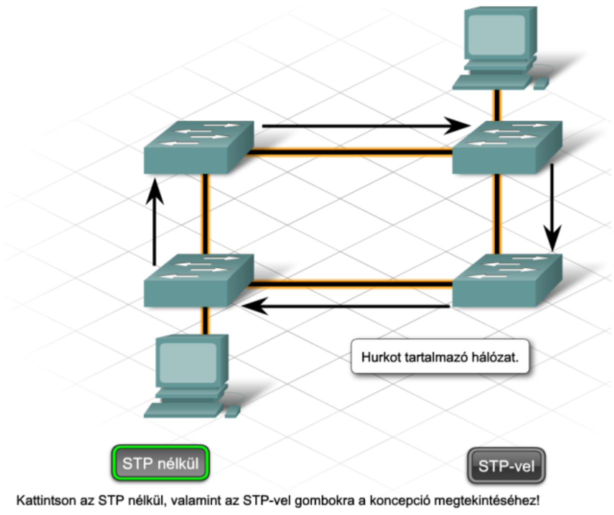
Redundáns hálózatokban előfordulhat, hogy a kapcsoló egy állomás elhelyezkedéséről rossz információt tanul meg. Ha létezik hurok, akkor a kapcsoló egy állomás MAC-címét akár két külön porttal is összefüggésbe hozhatja. Ez nem egyértelmű helyzetet és az optimálistól elmaradó kerettovábbítást okozhat.

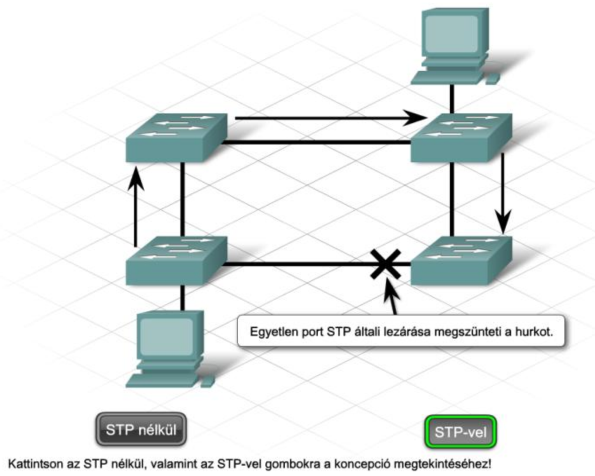
3.2.2 Feszítőfa protokoll (Spanning tree protocol, STP)

A feszítőfa protokoll kapcsolt hálózatok redundáns összeköttetéseinek letiltására szolgál. Az STP hurkok nélkül biztosítja a megbízhatóság növeléséhez szükséges redundanciát.

Az STP egy nyílt szabványú protokoll, melyet kapcsolt környezetben, hurokmentes logikai topológia létrehozására használnak.

Az STP egy minimális konfigurálást igénylő, lényegében önállóan működő protokoll. Azok a kapcsolók, melyeken engedélyezett az STP az első bekapcsoláskor ellenőrzik a kapcsolt hálózatok esetleges hurkait. Hurok észlelésekor letiltják az érintett portok valamelyikét, míg a többi porton aktív marad a kerettovábbítás.





Az STP a hálózat összes kapcsolóját egy faszerkezetű, kiterjesztett csillag topológiájú hálózattal kapcsolja össze. Ezek a kapcsolók folyamatosan ellenőrzik a hálózatot annak érdekében, hogy ne alakulhassanak ki hurkok és a portok megfelelően működjenek.
A kapcsolási hurkok kialakulásának megelőzésére az STP az alábbiakat teszi:

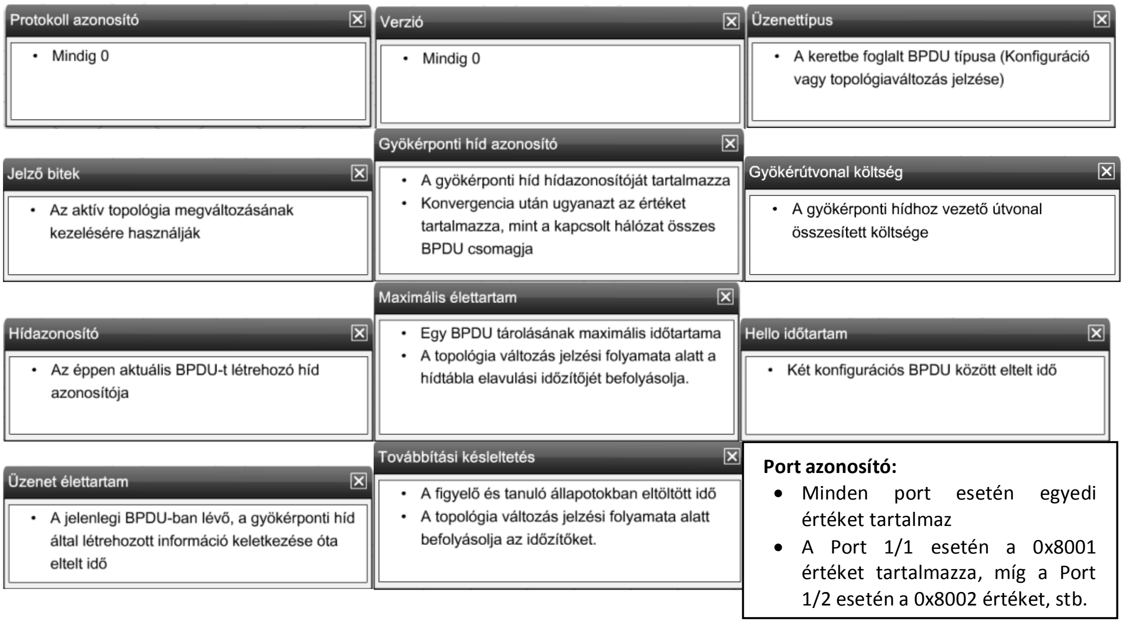
- Bizonyos interfészeket készenléti vagy lezárt állapotba helyez
- A többi interfészt továbbító állapotban hagyja
- Ha egy továbbító útvonal elérhetetlenné válik, akkor a hálózat újrakonfigurálásával a megfelelő készenléti útvonalat aktiválja.

Az STP terminológiát követve a kapcsolót gyakran hídnak nevezik. Például a gyökérponti híd az STP topológia elsődleges kapcsolója, vagyis központi pontja. A gyökérponti híd úgynevezett híd-protokoll adategységek (Bridge Protocol Data Unit, BPDU) segítségével kommunikál a többi kapcsolóval. A gyökérponti kapcsoló két másodpercenként csoportcímzéssel BPDU keretet küldik ki az összes többi kapcsolónak. A BPDU többek között a következő információkat tartalmazza:

- A BPDU-t küldő kapcsoló azonosítója
- A forrásport azonosítója
- A gyökérponti hídhoz vezető útvonal összesített költsége
- Az elévülési időzítők értéke
- A hello időzítők értéke

A BPDU felépítése

Protokoll azonosító	Verzió	Üzenettípus	Jelző bitek	Gyökérponti híd azonosító	Gyökérútvonal költség
Hídazonosító	Portazonosító	Üzenet élettartam	Maximális élettartam	Hello időtartam	Továbbítási késleltetés

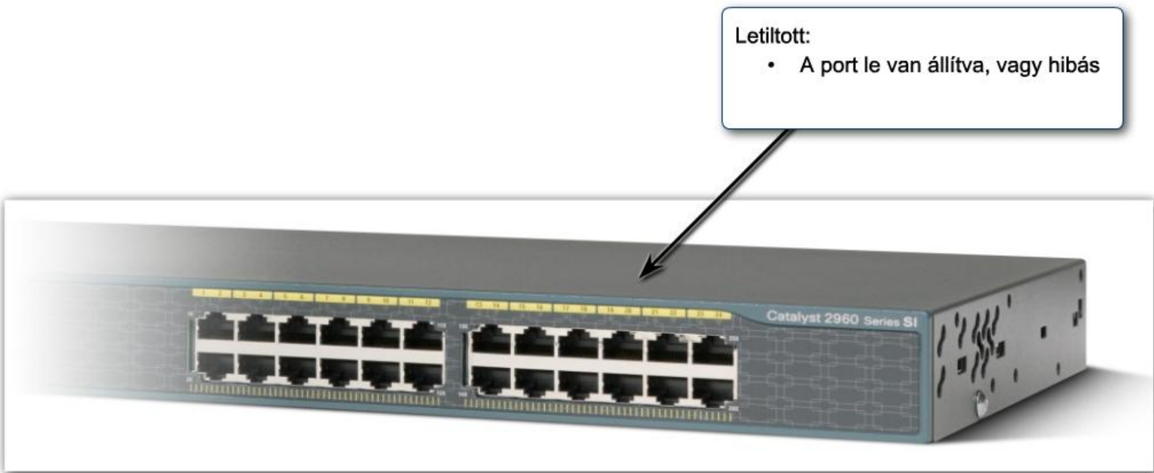


A kapcsoló elindítása után minden port végighalad a következő négy állapot sorozatán: lezárt, figyelő, tanuló és továbbító. Az ötödik, letiltott állapot jelzi, hogy a rendszergazda a portot letiltotta.

Miután a portok végigmennek ezeken az állapotokon, a kapcsoló port LED-jei villogó narancsszínűből folyamatos zöldre váltanak. Akár 50 másodpercbe is telhet, míg a portok az összes állapoton végighaladva továbbító módba kerülnek.

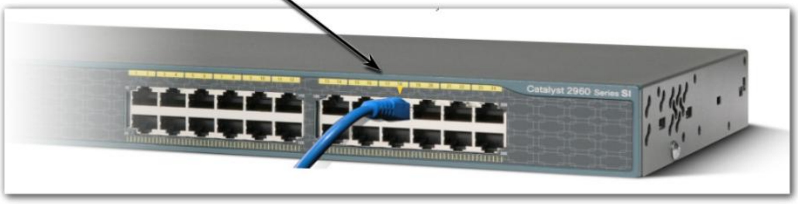
Bekapcsoláskor a portok lezárt állapotba kerülnek, azonnal megakadályozva a hurkok kialakulását. Ezután figyelő állapotba lépnek, ahol már fogadják a szomszéd kapcsolók BPDU kereteit. A kapott BPDU információ feldolgozása után a kapcsoló eldönti, hogy mely portok továbbíthatnak adatkereteket anélkül, hogy hurok alakulna ki. Ha egy port adatkereteket továbbíthat, akkor a port először tanuló módba, majd továbbító módba kerül.

A hozzáférési portok nem okozhatnak hurkokat a hálózatban, ezért ha állomás kapcsolódik rájuk rögtön továbbító módba kerülhetnek. A trönkportok esetén viszont fennáll a veszélye hurok kialakulásának, így azok vagy továbbító-, vagy lezárt állapotba kerülnek.



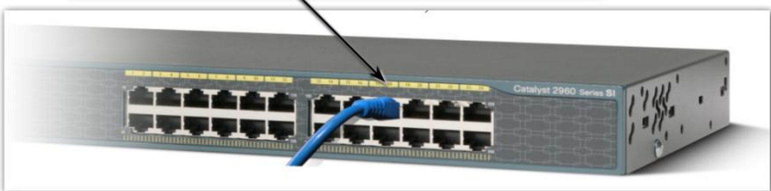
Lezárt:

- Borostyánsárgán világít
- BPDU-k fogadása
- Adatkeretek eldobása
- Nincs MAC-cím tanulás
- 20 másodperc elteltével figyelő állapotra vált



Figyelő:

- Borostyánsárgán villog
- BPDU-k figyelése
- Nincs kerettovábbítás
- Nincs MAC-cím tanulás
- Megtörténik annak meghatározása, hogy van-e a kapcsolónak egynél több trönkportja, mely hurkot hozhat létre
  - ha észlelt hurkot: visszavált lezárt állapotba
  - ha nincs hurok: tanuló állapotra vált
- 15 másodperc elteltével tanuló állapotba vált, ez az időtartam más néven a továbbítási késleltetés



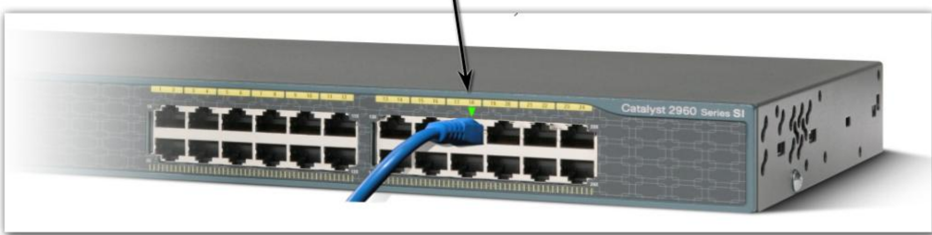
Tanuló:

- Borostyánsárgán villog
- BPDU-k feldolgozása
- A MAC-címek tanulása a fogadott forgalom alapján
- Nincs kerettovábbítás
- 15 másodperc elteltével továbbító állapotra vált



Továbbító

- Zölden villogó
- BPDU-k feldolgozása
- MAC-címek tanulása
- Keretek továbbítása

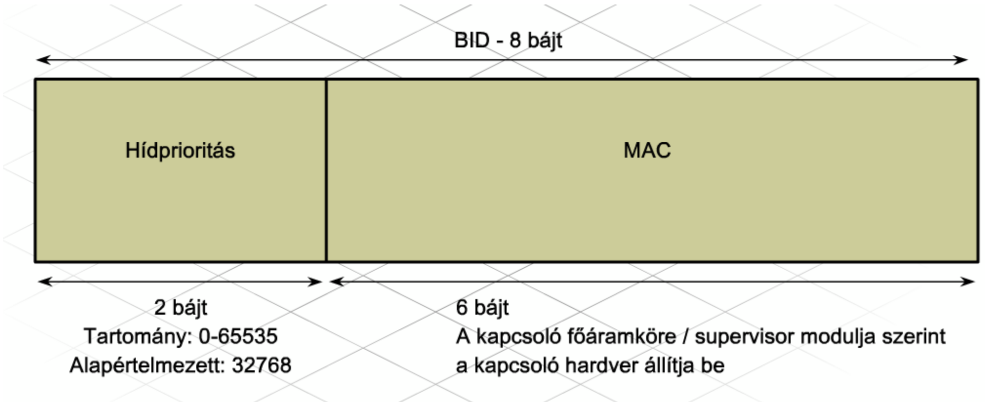


3.2.3 Gyökérponti hidak

Az STP működés első lépéseként a kapcsolók meghatározzák a hálózat központi pontját. Az STP ezt a központi pontot, más néven gyökérponti hídat (gyökérponti kapcsolót) használja annak eldöntésére, hogy mely portok kerüljenek lezárt és melyek továbbító állapotba. A gyökérponti híd a hálózat topológiájára vonatkozó információt tartalmazó BPDU-kat küld minden kapcsolónak. Ezen információk teszik lehetővé a hálózat újrakonfigurálását hiba esetén.

Minden hálózatban csak egy gyökérponti híd létezik, melyet a kapcsolók a hídazonosító (bridge ID, BID) alapján választanak ki. Ezt az azonosítót a híd prioritása és MAC-címe határozza meg.

A hídprioritás alapértelmezett értéke 32,768. Az AA-11-BB-22-CC-33 MAC-című kapcsoló alapértelmezett hídazonosítója 32768 : AA-11-BB-22-CC-33 lenne.



A gyökérponti híd a legkisebb hídazonosítójú kapcsoló. Mivel általában a kapcsolók az alapértelmezett értéket használják prioritásnak, így alapértelmezetten a legkisebb MAC-című kapcsoló lesz a gyökérponti híd.

Bekapcsoláskor mindegyik kapcsoló azt feltételezi, hogy ő a gyökérponti híd, ezért elkezdi a saját azonosítójával ellátott BPDU-k kiküldését. Ha S2 kisebb értékű azonosítót hirdet mint S1, akkor S1 nem folytatja saját azonosítójának hirdetését és elfogadja, hogy S2 a gyökérponti híd.

Az STP három különböző port típust definiál: gyökérponti port, kijelölt port és lezárt port.

Gyökérponti port

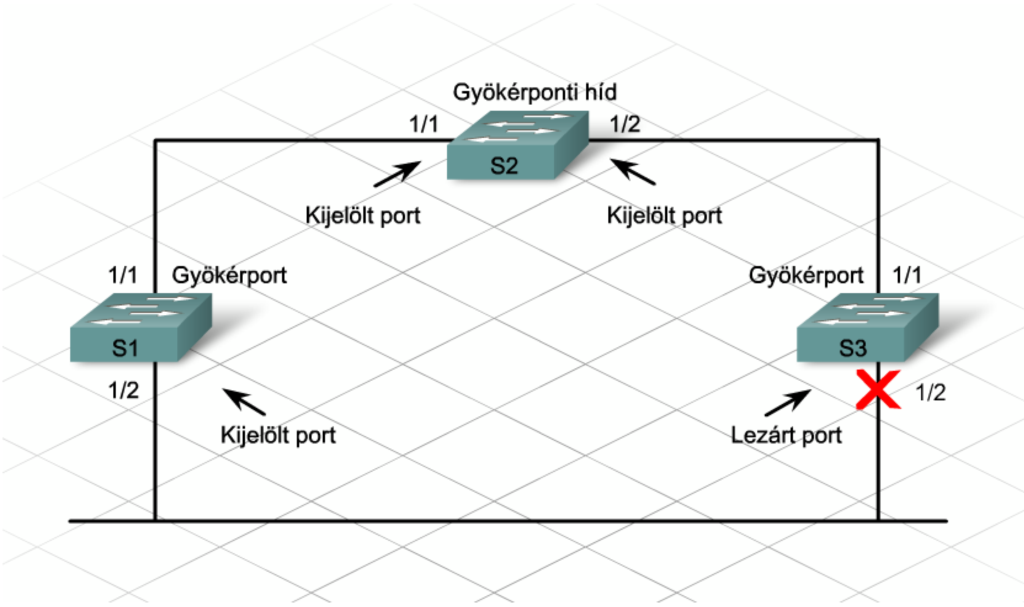
Egy kapcsoló azon portja amelyből a legkisebb költségű útvonal vezet a gyökérponti kapcsolóhoz. A kapcsolók a gyökérponti kapcsolóhoz vezető útvonal összeköttetéseinek eredő költségértéke alapján határozzák meg a legkisebb költségű útvonalat.

Kijelölt port

Egy hálózatszegmens azon portja amelyen át az adott szegmens és gyökérponti híd közötti adatforgalom halad, de nem tartozik a legkisebb költségű útvonalhoz.

Lezárt port

Olyan port, mely nem továbbít adatforgalmat.



Az STP konfigurálása előtt a hálózati rendszergazda elemzi és teszteli a hálózatot, hogy a legmegfelelőbb kapcsoló legyen a feszítőfa gyökérpontja. Nem biztos ugyanis, hogy az a legoptimálisabb, ha a legkisebb MAC-című kapcsoló lesz a gyökérponti híd.

Egy központi elhelyezkedésű kapcsoló felel meg leginkább a gyökérponti híd funkciójának. A hálózat szélén elhelyezkedő gyökérponti híd ugyanis azt okozhatja, hogy az adatok hosszabb útvonalon jutnak el a célállomásig, mintha a gyökérponti híd központi elhelyezkedésű lenne.

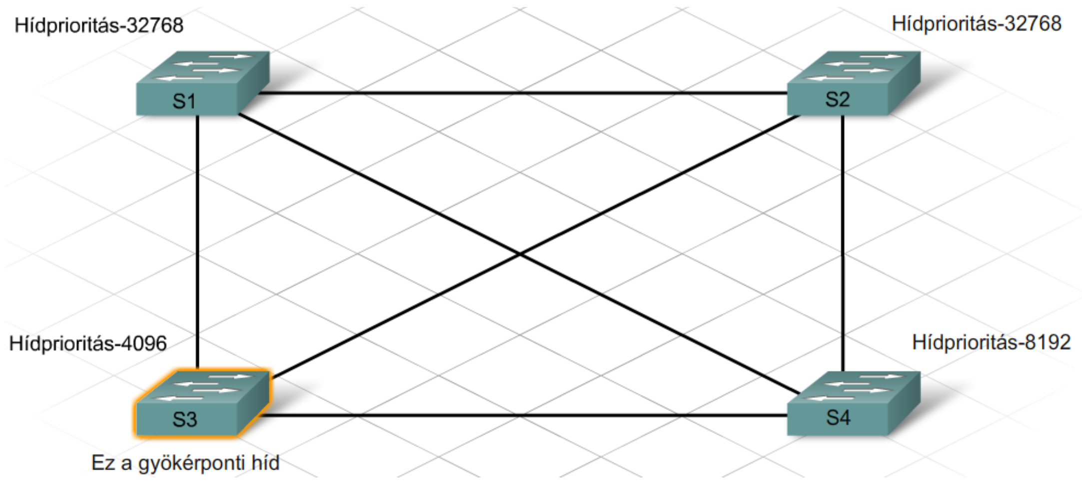
A gyökérponti híd funkciónak legmegfelelőbb kapcsoló azonosítóját a többihez képest kisebb prioritás értékkel kell konfigurálni. A bridge priority paranccsal állítható be a prioritás értéke. Ez 0-tól 65535-ig terjedhet, és 4096 egész számú többszörösének kell lennie. Az alapértelmezett érték 32768. Az alapértelmezett érték 32768.

A prioritás beállítása:

```
S3(config)#spanning-tree vlan 1 priority 4096
```

A prioritás alapértelmezett értékének visszaállítása:

```
S3(config)#no spanning-tree vlan 1 priority
```



3.2.4 Feszítőfa egy hierarchikus hálózatban

A gyökérponti híd, a gyökér-, a kijelölt- és a lezárt portok megválasztása után a gyökérponti híd két másodpercenként BPDU csomagokat küld a hálózaton keresztül minden kapcsolónak. Az STP folyamatosan figyeli ezeket a BPDU-kat az összeköttetés hibáinak és újabb hurkok keletkezésének elkerülése érdekében.

Ha egy összeköttetés meghibásodik, akkor az STP újból elvégzi a számításokat. Ennek eredményeként:

- Bizonyos lezárt portokat továbbító módba helyez
- Bizonyos továbbító portokat lezárt állapotba helyez
- Új feszítőfát készít a hurokmentes hálózat fenntartása érdekében

Az STP nem azonnal reagál a változásokra. Ha egy összeköttetés meghibásodik, akkor az STP észreveszi a hibát és kiszámolja a legjobb útvonalakat a hálózaton. Ez a számítás akár 30-50 másodpercet is igénybe vehet. Ezen idő alatt nincs adatforgalom az újraszámításban érintett portokon.

Bizonyos felhasználói alkalmazások esetében ez várakozási időtúllépést eredményezhet, ami a termelékenység és ezzel együtt a bevétel csökkenését eredményezheti. Gyakori STP újraszámolások negatív hatást gyakorolnak a hálózat működésére.

Ha nagy forgalmat bonyolító kiszolgáló csatlakozik egy porthoz, akkor ezen port újraszámolása esetén a kiszolgáló akár 50 másodpercig is elérhetetlenné válhat. Elképzelni is nehéz, hogy mennyi tranzakció veszik el a kiesett időintervallum alatt.

Stabil hálózatban az STP újraszámolások nem túl gyakoriak. Instabil hálózatban fontos a kapcsolók stabilitásának és konfiguráció változásainak ellenőrzése. Az STP újraszámolások egyik leggyakoribb oka a kapcsoló hibás tápellátása. A hibás tápellátás az eszköz váratlan újraindulását eredményezheti.

Az STP többirányú továbbfejlesztése is hozzájárul ahhoz, hogy az újraszámolás miatt fellépő kiesés időtartama csökkenjen.

PortFast

Az STP PortFast egy hozzáférési port számára lehetővé teszi, hogy a figyelő és tanuló állapotok kihagyásával rögtön továbbító módba kerüljön. A csupán egyetlen állomás vagy kiszolgáló kapcsolódását biztosító hozzáférési portokon beállitott PortFast móddal elérhető, hogy ezen eszközök még az STP konvergálása előtt csatlakozzanak a hálózathoz.

UplinkFast

Egy összeköttetés vagy kapcsoló meghibásodása, illetve az STP újrakonfigurálása esetén az STP UplinkFast felgyorsítja az új gyökérport kiválasztását. A gyökérport az STP normális működésétől eltérően, a figyelő- és tanuló állapotok kihagyásával rögtön továbbító módba kerül.

BackboneFast

A BackboneFast gyors konvergenciát biztosít a feszítőfa topológia megváltozásakor. Gyorsan visszaállítja a gerinchálózati összeköttetéseket. Az elosztási és a központi rétegben használják, ahol több kapcsoló csatlakozik egymáshoz.

Mivel a PortFast, UplinkFast és a BackboneFast a Cisco saját fejlesztései, így más gyártmányú kapcsolók esetén nem alkalmazhatóak. Ezen felül mindhárom funkció külön konfigurálást igényel.

Számos hasznos parancs létezik a feszítőfa protokoll helyes működésének ellenőrzésére.

`Show spanning-tree` – A gyökérponti híd azonosítóját, a hídazonosítót és a portok állapotát jeleníti meg

`Show spanning-tree summary` – A portok állapotáról ad összefoglaló információt

`Show spanning-tree root` – A gyökérponti híd állapotát és konfigurációját jeleníti meg

`Show spannig-tree detail` – Részletes információt nyújt a portokról

`Show spanning-tree interface` - Az STP interfészek állapotát és konfigurációját jeleníti meg

`Show spanning-tree blockedports` - Megmutatja a lezárt portokat

3.2.5 Gyors feszítőfa protokoll (Rapid spannig tree protocol, RSTP)

Amikor az IEEE kifejlesztette az eredeti 802.1D Feszítőfa protokollt (STP), akkor még 1-2 perc helyreállítási idő elfogadható volt. Manapság a 3. rétegű kapcsolás és a fejlettebb irányító protokollok gyorsabb alternatív útvonalat biztosítanak a célállomáshoz. A késleltetésre érzékeny forgalom, mint például hang- és videó átvitel a kapcsolt hálózatok gyors konvergenciáját igénylik, lépést tartva az újabb technológiák elvárásaival.

Az IEEE 802.1w szabványaként ismert gyors feszítőfa protokoll (RSTP) jelentősen felgyorsítja a feszítőfa újraszámolását. Eltérően a PortFast, UplinkFast és BackboneFast funkcióktól az RSTP nem cégorientáltan zárt protokoll.

Az RSTP a kapcsolók között duplex, pont-pont összeköttetést igényel a legnagyobb újrakonfigurálási sebesség eléréséhez. Az RSTP-vel a feszítőfa újrakonfigurálása kevesebb, mint 1 másodperc alatt megtörténik, eltérően a hagyományos STP-től, ahol ez akár 50 másodperc is lehet.

Az RSTP használatakor nincs szükség az olyan funkciókra, mint a PortFast és az UplinkFast. Az RSTP visszaállítható STP-re annak érdekében, hogy a szolgáltatás hagyományos eszközökkel együtt is működjön.

Az újraszámolási idő csökkentésére az RSTP mindössze háromra csökkenti a port állapotok számát: eldobó, tanuló és továbbító. Az eldobó állapot az eredeti STP három állapotához, a lezárt-, a figyelő- és a letiltott állapotokhoz hasonlítható.

Az RSTP bevezeti az aktív topológia fogalmát. Minden nem eldobó állapotban lévő port az aktív topológia része, és azonnal továbbító módba kerül.

3.3 VLAN-ok konfigurálása

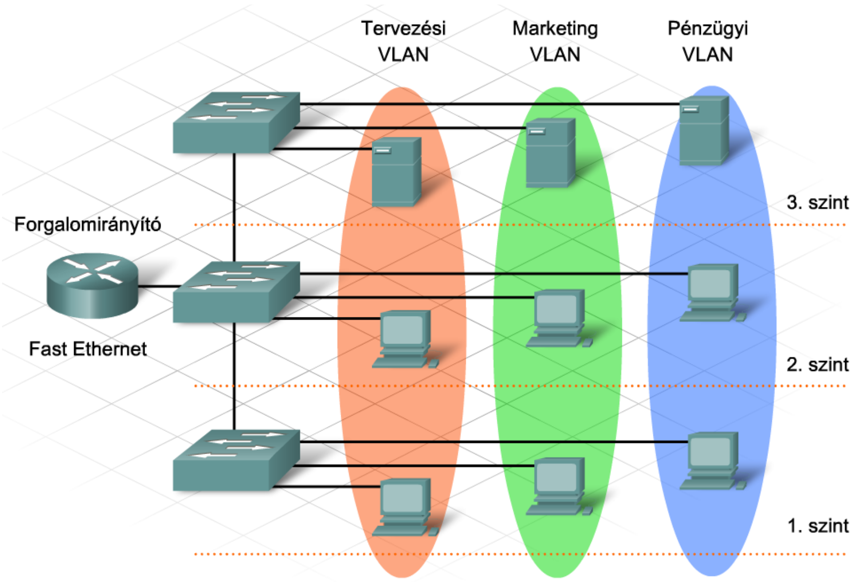
3.3.1 Virtuális LAN

A második rétegbeli kapcsolókhoz csatlakozó állomások és kiszolgálók azonos szegmenshez tartoznak, ami felvet két lényeges problémát:

- A kapcsolók az üzenetszórást minden portjukon kiküldik, így feleslegesen használják a sávszélességet. A kapcsolóhoz csatlakozó eszközök számának növelésével nő az üzenetszórások száma, és ezáltal növekszik a sávszélesség használat.
- Minden, a kapcsolóhoz csatlakozó eszköz továbbíthat és fogadhat kereteket minden más ide csatlakozó eszköztől.

A hálózattervezés általánosan alkalmazott gyakorlata szerint az üzenetszórásokat a hálózat lehető legszűkebb területén belül kell tartani. Üzleti megfontolások miatt bizonyos állomásoknak minden más állomást el kell érniük, míg más állomásoknál ez szükségtelen. Például a könyvelési kiszolgálót valószínűleg csak a könyvelési osztály tagjainak kell elérniük. Kapcsolt hálózatban az üzenetszórások korlátozása és az azonos felhasználási területhez tartozó állomások csoportosítása érdekében virtuális helyi hálózatok (VLAN - virtual local area network) hozhatók létre.

A VLAN egy logikai üzenetszórási tartomány, mely több fizikai LAN szegmensre is kiterjedhet. Lehetőséget nyújt a rendszergazdáknak az állomások logikai csoportosítására a fizikai elhelyezkedés figyelembevétele nélkül, például projektcsoportok vagy alkalmazási terület alapján.



A következő példa rávilágíthat a fizikai és a virtuális, más néven logikai hálózatok közötti különbségre:

Egy iskola tanulóit két csoportra osztjuk. Az egyik tagjai piros, míg a másik csoport tagjai kék azonosító kártyát kapnak. A legfontosabb követendő elv, hogy a piros kártyások csak piros kártyásokkal, a kékek pedig csak kékekkel beszélhetnek. Ily módon a tanulók két logikailag elkülönülő, virtuális csoporthoz vagy VLAN-hoz tartoznak.

E logikai csoportosítást használva, az üzenetszórás csak a piros kártyások körében terjed el, még ha a két csoport fizikailag egy iskolához tartozik is.

A példa rámutat a virtuális helyi hálózatok egy további jellemzőjére is, nevezetesen, hogy az üzenetszórások a VLAN-ok között nem kerülnek továbbításra, hanem a VLAN-on belül maradnak.

Minden VLAN önálló helyi hálózatként működik. Egy vagy több kapcsolón ível át, lehetőséget teremtve az állomásoknak, hogy úgy működjenek, mintha azonos hálózati szegmenshez tartoznának.

A VLAN két legfontosabb feladata:

- Az üzenetszórások VLAN-on belül tartása.
- Az eszközök csoportosítása. Az egyik VLAN-hoz tartozó állomások láthatatlanok maradnak egy másik VLAN állomásai számára.

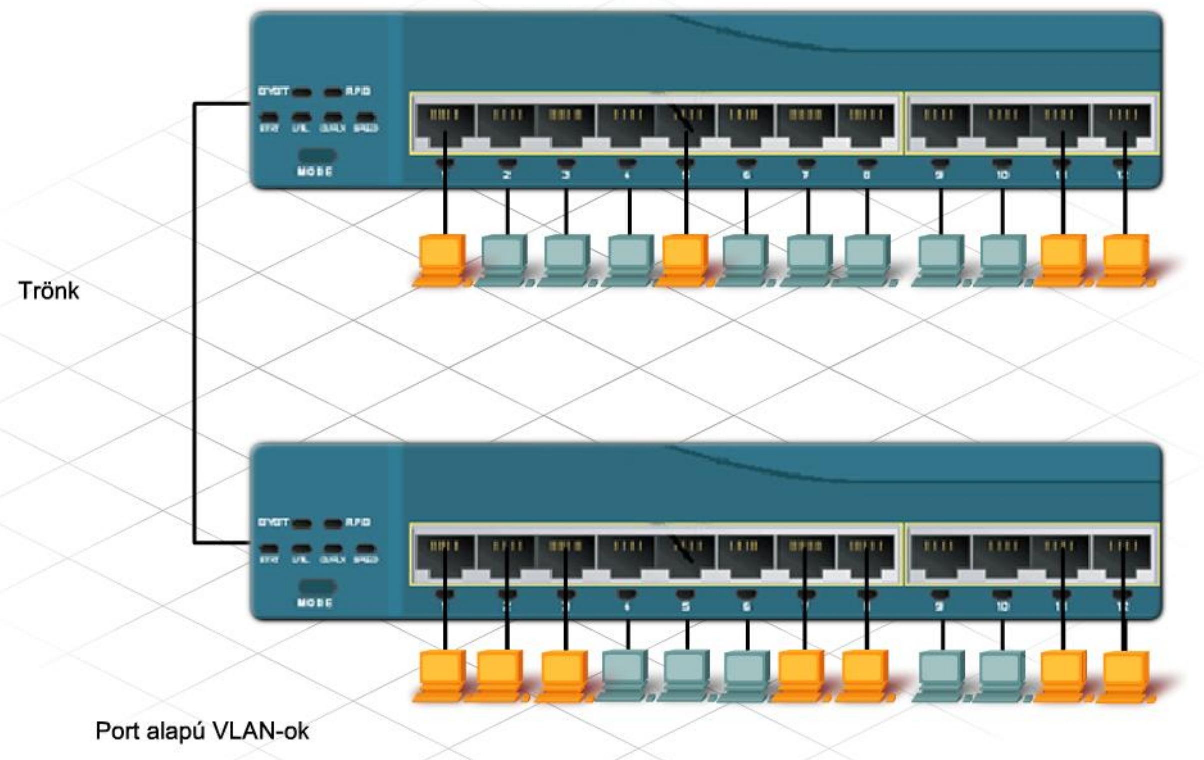
Virtuális helyi hálózatok közötti adattovábbításhoz harmadik rétegbeli eszköz szükséges.

Kapcsolt hálózatban az eszközök elhelyezkedésük, MAC-címük, IP-címük vagy leggyakrabban használt alkalmazásaik alapján lehetnek egy adott VLAN tagjai. A hozzárendelést a rendszergazda elvégezheti statikusan vagy dinamikusan.

Statikus VLAN tagság estén a rendszergazda manuálisan rendel minden kapcsolóportot egy meghatározott VLAN-hoz. Például az Fa0/3-as portot hozzárendelheti a 20-as VLAN-hoz, így bármelyik eszközt is csatlakoztatunk ide, az automatikusan a 20-as VLAN tagjává válik.

A VLAN tagság beállításának ez a módszere a legkönnyebb és a legelterjedtebb, annak ellenére, hogy a hozzáadás, az eltávolítás vagy a változtatás ekkor jár a legtöbb adminisztrációval. Például, ha egy állomást egy VLAN-ból egy másikba szeretnénk áthelyezni, akkor vagy a portot kell manuálisan újrakonfigurálni, vagy a munkaállomás kábelét kell egy másik porthoz csatlakoztatni.

A VLAN-tagság a felhasználó elől teljes mértékben rejtve marad. A kapcsoló egyik portjához csatlakozó eszközön dolgozó felhasználónak nincs tudomása arról, melyik VLAN-hoz tartozik.



Dinamikus VLAN-tagság beállításánál egy VLAN-tagságot kezelő kiszolgáló (VMPS - VLAN management policy server) alkalmazása szükséges, amely nyilvántartja a MAC-címek és VLAN-ok közötti megfeleltetéseket. Amikor egy eszköz egy kapcsolóporthoz csatlakozik, a VMPS megkeresi adatbázisában az adott MAC-címet, és a használt portot átmenetileg a megfelelő VLAN-hoz rendeli.

A dinamikus VLAN-tagság több szervezést és beállítást igényel, azonban jóval rugalmasabb rendszert hoz létre a tagságok kezelésére, mint a statikus módszer. A hozzáadás, a változtatás és az eltávolítás automatikusan megy végbe, és nincs szükség rendszergazdai beavatkozásra.

Megjegyzés: Nem minden Catalyst kapcsoló támogatja a VMPS alkalmazását.

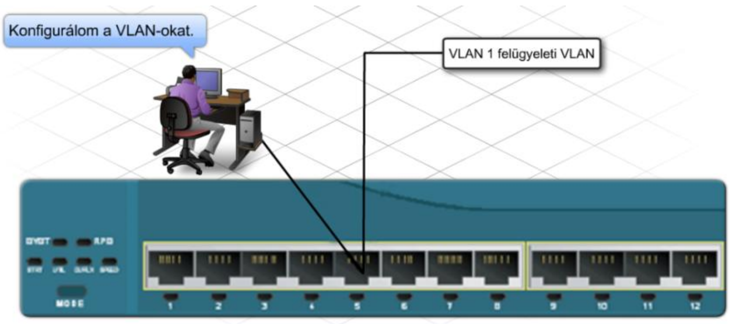
3.3.2 Virtuális helyi hálózat konfigurálása

VLAN-ok létrehozása akár statikusan, akár dinamikusan történik, maximális számuk a kapcsoló típusától és az IOS-től függ. Alapértelmezés szerint az 1-es VLAN a felügyeleti VLAN.

A kapcsoló távoli konfigurálására a felügyeleti VLAN IP-címét használhatja a rendszergazda. Távoli elérés esetén beállíthatja és karbantarthatja a VLAN-konfigurációkat.

A felügyeleti VLAN szolgál a más hálózati eszközökkel folytatott Cisco Discovery Protocol (CDP) és VLAN Trunking Protocol (VTP) információcserére is.

Egy VLAN létrehozásakor egy számot és egy nevet kell megadni. A VLAN száma, az 1-es VLAN-t leszámítva, bármely érték lehet a kapcsolón engedélyezett tartományból. Némely kapcsoló megközelítőleg 1000 VLAN létrehozását teszi lehetővé, míg mások akár a 4000-et is támogatnak. A VLAN-ok elnevezése a hálózat üzemeltetőinek erre vonatkozó gyakorlatát követi.



VLAN-ok létrehozására globális konfigurációs módban az alábbi parancsok használhatók:

```
Switch(config)#vlan vlan_szám

Switch(config-vlan)#name vlan_név

Switch(config-vlan)#exit
```

Az egyes portok a már létező VLAN-okhoz rendelhetők. Kezdetben alapértelmezés szerint minden port az 1-es VLAN-hoz tartozik. A portok hozzárendelése történhet egyesével vagy csoportosan.

Több port egyidejű VLAN-hoz rendelésére az alábbi parancsok használhatók:

```
Switch(config)#interface fa0/port_szám

Switch(config-if)#switchport access vlan vlan_szám
```

```
Switch(config-if)#exit
```

Több port egyidejű VLAN-hoz rendelésére az alábbi parancsok használhatók:

```
Switch(config)#interface range fa0/tartomány_kezdete - tartomány_vége
```

```
Switch(config-if)#switchport access vlan vlan_szám
```

```
Switch(config-if)#exit
```

A VLAN-ok ellenőrzése, karbantartása és hibaelhárítása érdekében elengedhetetlen a Cisco IOS rendelkezésre álló `show` parancsainak megértése.

VLAN-ok ellenőrzésére és karbantartására az alábbi parancsok használhatók:

```
show vlan
```

- Részletes listát jelenít meg a kapcsoló jelenleg aktív VLAN-jairól, feltüntetve azok nevét, számát és a hozzárendelt portokat.
- STP statisztikát jelenít meg, ha a kapcsoló VLAN-alapú STP-re van beállítva.

```
show vlan brief
```

- Összesített listát jelenít meg kizárólag az aktív VLAN-okról és az azokhoz rendelt portokról

```
show vlan id azonosító_szám
```

- Az azonosítószámával (ID) megadott VLAN-ra vonatkozóan jelenít meg információkat.

```
show vlan name vlan_szám
```

- A nevével megadott VLAN-ra vonatkozóan jelenít meg információkat.

Egy szervezetnél gyakran előfordul, hogy egy osztály vagy egy projektcsapat összetétele megváltozik: új munkatársak kerülhetnek a csapathoz, míg mások munkahelye megszűnhet vagy új helyre kerülhet. Az ilyen gyakori változások szükségessé teszik a VLAN-ok karbantartását, beleértve egy vagy több VLAN törlését vagy portok hozzárendelését egy másik virtuális hálózathoz.

A VLAN-ok törlése és a VLAN-hoz tarozó port-hozzárendelések megszüntetése két, egymástól jól elkülöníthető rendeltetésű és eredményű művelet. Amikor egy port, egy meghatározott VLAN-hoz tartozó hozzárendelését megszüntetjük, visszakerül az 1-es VLAN-ba. Amikor egy VLAN-t törlünk, minden hozzátartozó port inaktívvá válik, mivel egyetlen VLAN-hoz sem tartozik.

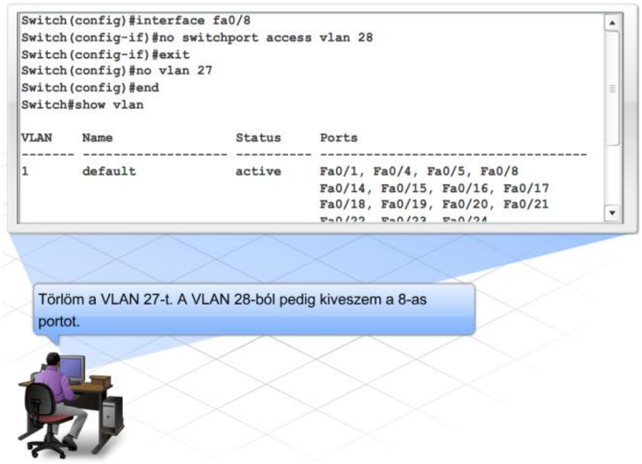
VLAN törlése:

```
Switch(config)#no vlan vlan_szám
```

Port kivétele egy meghatározott VLAN-ból:

```
Switch(config)#interface fa0/port_szám
```

```
Switch(config-if)#no switchport access vlan vlan_szám
```



3.3.3 VLAN-ok azonosítása

Egy adott VLAN-hoz tartozó eszközök csak az azonos VLAN-hoz tartozókkal képesek közvetlenül kommunikálni, függetlenül attól, hogy ugyanahhoz vagy másik kapcsolókhoz csatlakoznak-e.

A kapcsoló minden portjához egy meghatározott VLAN-t rendel. Amikor egy keret érkezik a portra, a kapcsoló bejegyzi az Ethernet keretbe a VLAN azonosítóját (VID - VLAN ID). A VID Ethernet kerethez történő hozzáadását keretcímkézésnek (frame tagging) nevezik. A leggyakrabban alkalmazott címkézési szabvány az IEEE 802.1Q.

A 802.1Q szabvány, röviden dot1q, egy 4-bájtos mezőt illeszt az Ethernet keretbe, a forráscím és a típus/hossz mező közé.

Mivel az Ethernet keret legkisebb mérete 64 bájt, a legnagyobb mérete pedig 1518 bájt lehet, a felcímkézett keret mérete elérheti az 1522 bájtot.

A keretek többek között az alábbi mezőket tartalmazzák:

- a forrás és a cél MAC-címe
- a keret hossza
- hasznos adat
- keretellenőrző összeg (FCS - frame check sequence)

Az FCS mező a keret hibaellenőrzését tesz lehetővé, biztosítva az összes bit sértetlen kézbesítését.

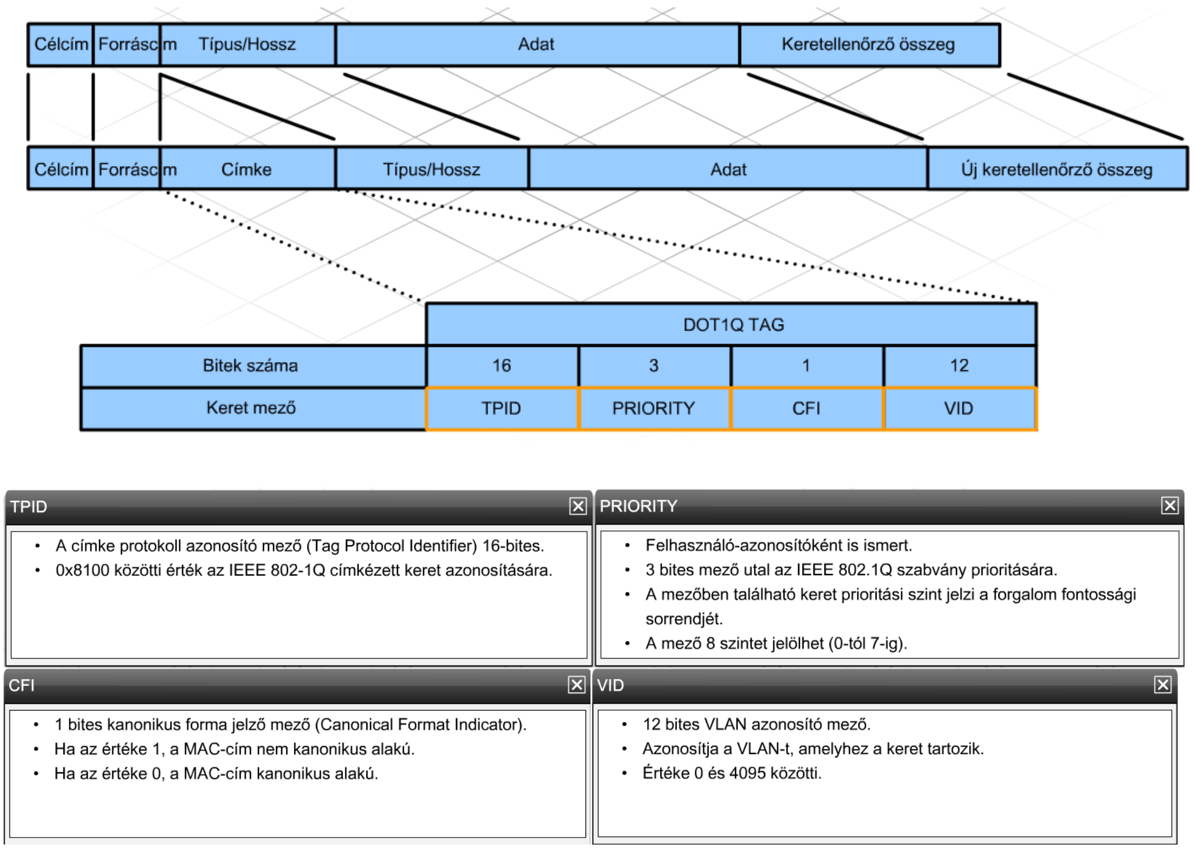
A címkézési mező megnöveli az Ethernet keret minimális hosszát 64 bájtról 68-ra, és a maximális hosszát 1518-ról 1522 bájtra. A bitszám megváltozásának következményeként a kapcsoló újraszámítja a keretellenőrző összeget.

Ha egy 802.1Q protokollnak megfelelő port egy másik ugyanilyen porthoz csatlakozik, a VLAN címkézési információ a két port között továbbítódik.

Ha a kapcsolódó port nem felel meg a 802.1Q protokollnak, a VLAN címkét a kapcsoló eltávolítja, mielőtt a keret az átviteli közegre kerülne.

Ha 802.1Q protokollt nem támogató eszköz vagy port 802.1Q keretet kap, a címkézési adatot figyelmen kívül hagyja, és a keretet egy szokványos Ethernet keretként továbbítja a második

rétegben. Ebből következően további második rétegbeli közbülső eszközök (például kapcsolók és hidak) helyezhetők el a trönk vonalon. A 802.1Q keretcímkézés kezeléséhez ezeknek az eszközöknek 1522 bájtos vagy nagyobb keretek kezelésére is képesnek kell lenniük.



3.4 A trönkölés és VLAN-ok közötti forgalomirányítás

3.4.1 Trönkportok

A VLAN-oknak három fő feladatuk van:

- az üzenetszórási tartományok korlátozása
- a hálózat teljesítményének növelése
- alapszintű védelem biztosítása

A VLAN-ok összes előnyének kihasználása érdekében a VLAN-ok több kapcsolóra is kiterjeszthetők.

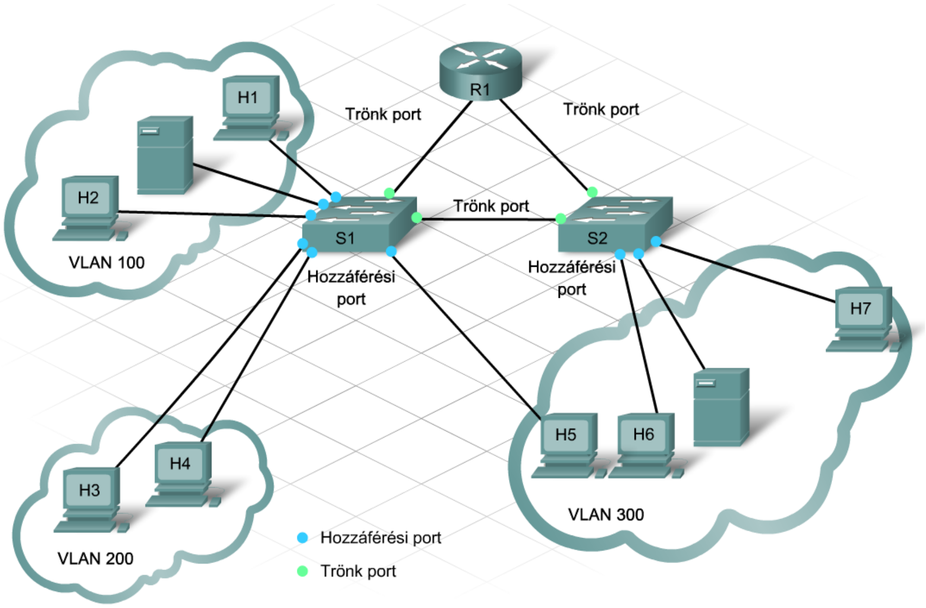
A kapcsoló portjai két különböző feladat ellátására konfigurálhatók: vagy hozzáférési portok, vagy trönkportok lesznek.

Hozzáférési port

A hozzáférési port kizárólag egy VLAN-hoz tartozik. Általában egyetlen eszköz, asztali gép vagy kiszolgáló kapcsolódik ehhez a porthoz. Ha hubon keresztül több állomás is csatlakozik hozzá, mindegyik ugyanannak a VLAN-nak a tagja lesz.

Trönkport

A trönkport két kapcsolót vagy más hálózati eszközt összekötő pont-pont kapcsolat, mely több VLAN forgalmát továbbítja egyetlen kapcsolaton keresztül, lehetővé téve a VLAN-ok számára a teljes hálózat elérését. Trönkportokra van szükség, amennyiben különböző VLAN-okhoz tartozó eszközök közötti forgalmat kell továbbítani olyan környezetben, ahol egy kapcsoló egy másik kapcsolóhoz, kapcsoló forgalomirányítóhoz vagy kapcsoló egy 802.1Q trönkölést támogató hálózati kártyával rendelkező állomáshoz csatlakozik.



Trönkport nélkül minden egyes VLAN külön összeköttetést igényelne a kapcsolók között. Például egy vállalatnál 100 db VLAN 100 külön összeköttetést igényelne. Az ilyen elrendezés nehézkesen bővíthető és költséges. A trönk-kapcsolatok megoldást jelentenek a problémára azzal, hogy több VLAN forgalmát képesek szállítani egyetlen kapcsolaton keresztül.

Több VLAN forgalmának egyidejű szállítása egyetlen összeköttetésen a VLAN-ok azonosítását teszi szükségessé. A trönkportok támogatják a keretcímkézést, melynek során VLAN információk kerülnek a keretbe.

A IEEE 802.1Q a keretcímkézésre vonatkozó szabványos és elfogadott eljárás. A Cisco kifejlesztett egy saját keretcímkézési protokollt is, kapcsolók közötti összeköttetés (ISL - Inter-Switch Link) néven. A nagyteljesítményű kapcsolók, mint például a Catalyst 6500-as sorozat eszközei, mindkét keretcímkézési protokollt támogatják, azonban a legtöbb LAN kapcsoló, mint például a 2960-as, csak a 802.1Q protokollt támogatja.

Alapértelmezés szerint a kapcsolók portjai hozzáférési portok. Trönkport konfigurálására az alábbi parancsok használhatók:

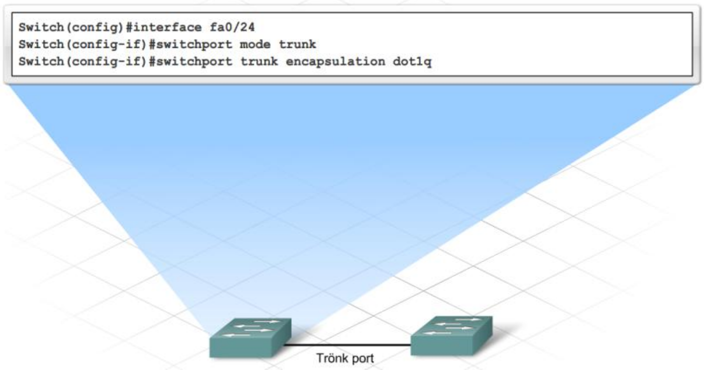
```
Switch(config)#interface fa0/port_szám

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk encapsulation {dot1q | isl | negotiate}
```

A 802.1Q és az ISL protokollokat egyaránt támogató kapcsolók esetén az utolsó parancssor is szükséges. A 2960-as kapcsoló esetén ez felesleges, hiszen ez csak a 802.1Q protokollt támogatja.

A „negotiate” (egyeztet) paraméter a legtöbb kapcsolón alapértelmezett. Ez a beállítás a szomszédos kapcsolók közötti beágyazás típusának automatikus észlelését írja elő.



Az újabb kapcsolók képesek az összeköttetések másik végpontjának beállításait felismerni, így a csatlakozó eszköz szerint konfigurálják a kapcsolatot trönk, illetve hozzáférési portnak.

```
Switch(config-if)#switchport mode dynamic {desirable | auto}
```

„desirable” (elvárt) módban a port trönkport lesz, ha az összeköttetés túlsó vége trunk, desirable, vagy auto módban van.

„auto” módban a port trönkport lesz, ha az összeköttetés túlsó vége trunk vagy desirable módban van.

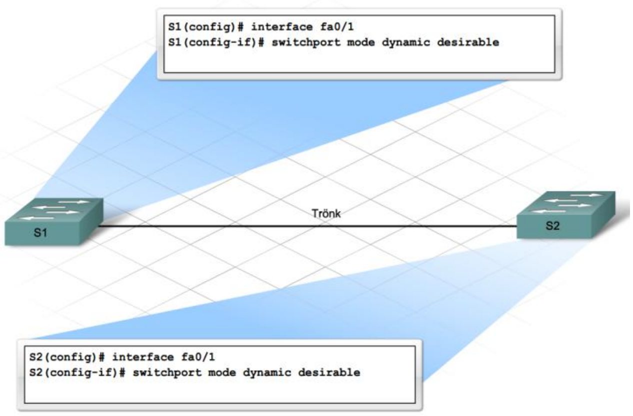
Ha egy trönkportot ismét hozzáférési portra szeretnénk konfigurálni, az alábbi parancsok használhatók:

```
Switch(config)#interface fa0/port_szám
```

```
Switch(config-if)#no switchport mode trunk
```

vagy

```
Switch(config-if)#switchport mode access
```



3.4.2 Több kapcsolóra kiterjedő VLAN-ok

A trönkölési eljárás lehetővé teszi több VLAN forgalmának továbbítását egyetlen porton keresztül.

Mindkét végén 802.1Q címkézésre beállított összeköttetés esetén minden keret egy 4-bájtos címkézési mezővel egészül ki. Ez a mező tartalmazza a VLAN azonosítót (VLAN ID).

Amikor egy kapcsoló címkézett keretet fogad egy trönkportján, egy hozzáférési portra történő továbbítás előtt eltávolítja a címkét. A továbbítást csak akkor hajtja végre, ha a port a címkézési mezőben feltüntetett VLAN-nak tagja.

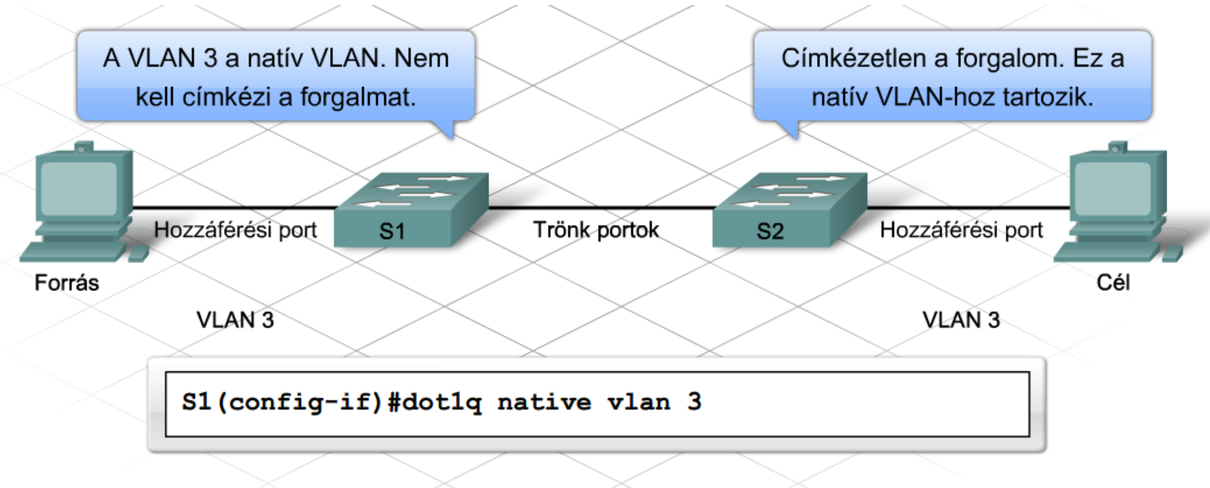
Bizonyos forgalom-tipusok keretei esetén elkerülhetetlen, hogy azok VLAN ID nélkül haladjanak át egy 802.1Q összeköttetésen. Az ilyen forgalmat címkézetlen forgalomnak nevezik. Ilyen például a CDP és a VTP protokollok forgalma, valamint bizonyos típusú hangátviteli forgalom. A címkézetlen forgalom késleltetése kisebb, mivel ilyenkor kimarad a VLAN ID kezelés fázisa.

A címkézetlen forgalom lehetővé tétele érdekében egy speciális VLAN, az úgynevezett natív VLAN alkalmazható. Egy 802.1Q trönkportra érkező címkézetlen forgalom a natív VLAN-hoz fog tartozni. A Cisco Catalyst kapcsolókon alapértelmezés szerint az 1-es VLAN a natív VLAN.

Bármely VLAN beállítható natív VLAN-nak. Meg kell bizonyosodni ugyanakkor arról, hogy a trönkvonal mindkét végén egyformán van beállítva a natív VLAN. Ha különbözik a beállítás, hurok jöhet létre a feszítőfa kialakítása során.

Egy 802.1Q összeköttetéshez tartozó fizikai interfészen a natív VLAN beállítására az alábbi parancs alkalmazható:

```
Switch(config-if)#dot1q native vlan vlan-azonosító
```

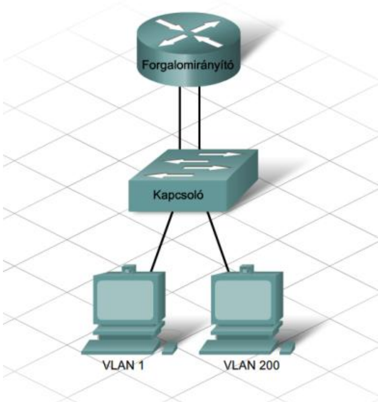


3.4.3 VLAN-ok közötti forgalomirányítás

Habár a VLAN-ok több kapcsolóra is kiterjedhetnek, csak az azonos VLAN-hoz tartozó tagok kommunikálhatnak közvetlenül egymással.

A különböző VLAN-ok között csak harmadik rétegbeli eszköz tud kapcsolatot teremteni. Ez az elrendezés lehetővé teszi a rendszergazda számára a VLAN-ok közötti forgalom szigorú ellenőrzését.

A VLAN-ok közötti forgalomirányítás megvalósításának egyik módja, amikor minden VLAN a harmadik rétegbeli eszköz egy-egy külön interfészéhez kapcsolódik.



A VLAN 1 akkor tudja elérni a VLAN 200-at, ha mindketten dedikált kapcsolattal rendelkeznek a forgalomirányító felé.

A különböző VLAN-ok közötti kapcsolat kialakításának másik módja alinterfészek alkalmazásával történik. Az alinterfészek egy fizikai interfész logikai felosztásából jönnek létre. Ebben az esetben minden VLAN-hoz egy alinterfészt kell konfigurálni.

Az alinterfészek alkalmazásával megvalósított VLAN-ok közötti (inter-VLAN) kommunikációhoz a kapcsolón és a forgalomirányítón egyaránt el kell végezni a megfelelő beállításokat.

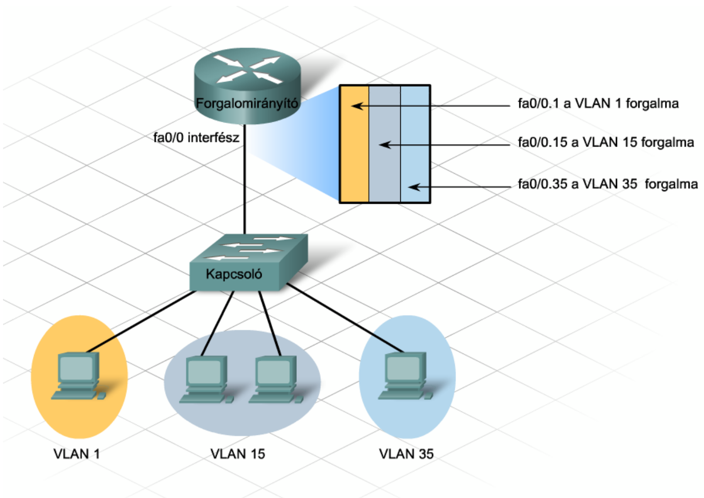
Kapcsoló

- Konfiguráljuk a kapcsoló interfészét 802.1Q trönkportra!

Forgalomirányító

- Válasszunk a forgalomirányítón egy minimum 100 Mbit/s sebességű Fast Ethernet interfészt!
- Konfiguráljunk alinterfészeket, és állítsuk be rajtuk a 802.1Q beágyazást!
- Konfiguráljunk minden VLAN-hoz egy alinterfészt!

Az alinterfészek alkalmazása lehetővé teszi, hogy minden VLAN-nak saját logikai útvonala és alapértelmezett átjárója legyen a forgalomirányítón.



Egy VLAN-ból történő adatküldés esetén az oda tartozó állomás az alapértelmezett átjáró beállított értékének megfelelően a csomagokat a forgalomirányítónak továbbítja. A VLAN-hoz rendelt alinterfész egyúttal alapértelmezett átjáróként fog működni az adott VLAN állomásai számára. A forgalomirányító meghatározza a cél IP-címet, majd kikeresi a hozzátartozó bejegyzést az irányítótáblában.

Ha a cél VLAN ugyanahhoz a kapcsolóhoz csatlakozik, mint a forrás VLAN, akkor a forgalomirányító visszairányítja a csomagot a kapcsoló felé a cél VLAN ID-nek megfelelő alinterfészt használva. Ezt a konfiguráció típust gyakran router-on-a-stick néven emlegetik.

Ha a forgalomirányító kimenő interfésze 802.1Q kompatibilis, a keret megtartja a 4-bájtos VLAN címkét. Ellenkező esetben a forgalomirányító eltávolítja a címkét a keretből, és visszaállítja az eredeti Ethernet formát.

VLAN-ok közötti forgalomirányítás konfigurálásához az alábbi lépések szükségesek:

1. Trönkport konfigurálása a kapcsolón.

```
Router(config)#interface fa2/0

Switch(config-if)#switchport mode trunk
```

2. IP-cím és alhálózati maszk nélküli interfész konfigurálása a forgalomirányítón.

```
Router(config)#interface fa1/0

Router(config-if)#no ip address

Router(config-if)#no shutdown
```

3. Minden VLAN-hoz alinterfész konfigurálása a forgalomirányítón. Az alinterfészeken 802.1Q beágyazás szükséges.

```
Router(config)#interface fa0.10/0

Router(config-subif)#encapsulation dot1q 10

Router(config-subif)#ip address 192.168.10.1 255.255.255.0
```

4. A VLAN-ok közötti forgalomirányítás beállításainak és működésének ellenőrzéséhez az alábbi parancsok használhatók:

```
Switch#show trunk

Router#show ip interfaces

Router#show ip interfaces brief

Router#show ip route
```

3.5 VLAN-ok kezelése vállalati hálózatokban

3.5.1 VLAN trönkprotokoll (VTP)

A hálózatok méretének és összetettségének növekedésével szükségszerűvé válik a VLAN-ok központi felügyelete. A VLAN-trönkprotokoll (VTP – VLAN Trunking Protocol) egy 2. rétegbeli üzenettovábbító protokoll, amely lehetővé teszi egy hálózati szegmensen a VLAN adatbázis megosztását és felügyeletét egy központi kiszolgálóról. A forgalomirányítók nem továbbítják a VTP frissítéseket.

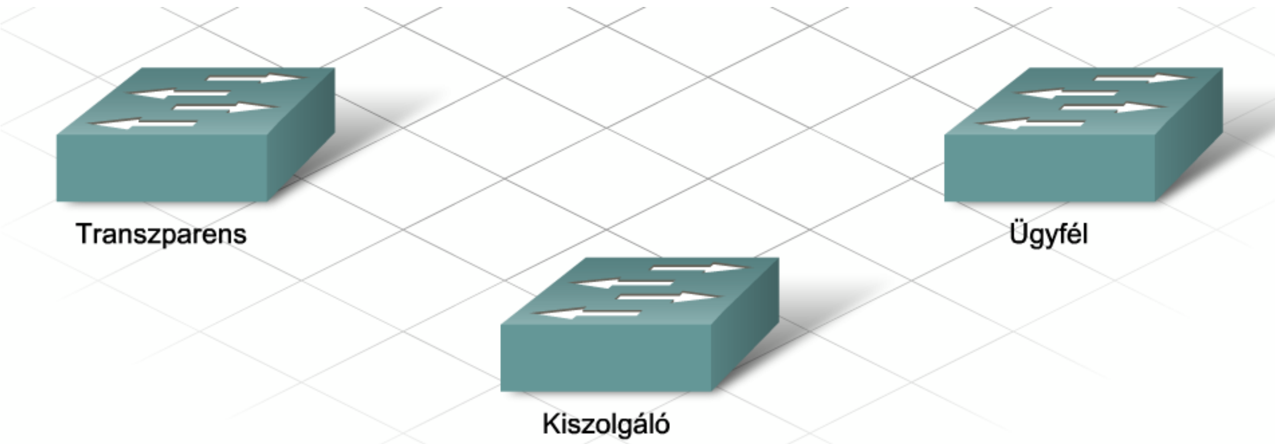
Amennyiben nincs lehetőség egy több száz VLAN-t tartalmazó vállalati hálózat automatizált felügyeletére, akkor minden kapcsolón minden VLAN-t kézzel kell beállítani, és a VLAN-okban bekövetkező minden változás is további kézi konfigurációt igényel. Egy hibásan leütött szám az egész hálózatra kiterjedő kapcsolathibát okozhat.

A Cisco ennek elkerülésére fejlesztette a ki a számos VLAN beállítási lehetőség automatikus elvégzésére szolgáló VTP protokollt. A VTP gondoskodik a VLAN konfiguráció egész hálózatra kiterjedő egységességének kialakításáról, és csökkenti a VLAN felügyelettel és megfigyeléssel járó feladatok számát.

A VTP egy ügyfél-kiszolgáló alapú üzenettovábbító protokoll, amely egy VTP tartományban VLAN-ok létrehozására, törlésére és átnevezésére szolgál. A közös felügyelet alá tartozó kapcsolók mindegyike egy tartomány része. Minden tartomány egyedi névvel rendelkezik. A VTP kapcsolók csak az ugyanahhoz a tartományhoz tartozó kapcsolóknak küldik el VTP üzeneteiket.

Két VTP változat létezik, az 1-es és a 2-es. Az 1-es változat az alapértelmezett, és nem kompatibilis a 2-es változattal. Minden kapcsolón ugyanazt a változatot kell beállítani.

A VTP három módban működik: kiszolgáló, ügyfél és transzparens. Alapesetben minden kapcsoló kiszolgáló módban van. A redundancia érdekében ajánlott legalább két kiszolgáló módú kapcsolót konfigurálni.



Transzparens

- Továbbítja a VTP hirdetményeket.
- A VTP üzenetekben szereplő információkat nem veszi figyelembe.
- Frissítési üzenet hatására nem változtatja meg adatbázisát.
- Saját VLAN adatbázisának változásairól nem küld frissítést.

Kiszolgáló

- A teljes tartományra vonatkozóan létrehoz, módosít és töröl VLAN-okat és VLAN konfigurációs paramétereket.
- A VLAN konfigurációs információkat az NVRAM-ba menti.
- VTP üzeneteket küld ki minden trönkportján.

Ügyfél

- Nem módosít, változtat és töröl VLAN információkat.
- A kiszolgálótól kapott VLAN változások alapján módosítja saját adatbázisát.
- VTP üzeneteket küld ki minden trönkportján.

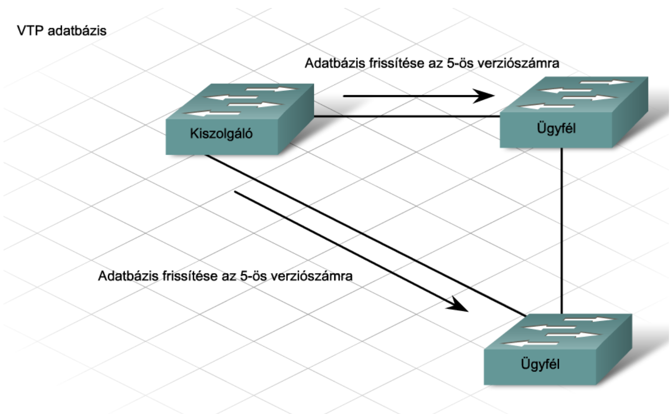
Minden VTP kapcsoló a trönk portjain küldi VTP hirdetményeit, melyek tartalmazzák a felügyeleti tartomány, a konfiguráció verziószám adatokat és az összes VLAN paraméterét. A kapcsolók ezeket a hirdetménykereteket egy csoport címre küldik, amit így minden szomszédos eszköz megkap.

Minden VTP kapcsoló az NVRAM-ban tárolja VLAN adatbázisát, ami tartalmaz egy verziószámot. Ha a kapcsoló az adatbázisban tároltnál nagyobb verziószámú hirdetményt kap, akkor frissíti VLAN adatbázisát az új információkkal.

A VTP konfiguráció verziószáma 0-ról indul, és minden változáskor eggyel nő. Maximális értéke 2 147 483 648, amit elérve visszaáll 0-ra. A kapcsoló újraindítása szintén 0-ra állítja a verziószámot.

A verziószám akkor okozhat gondot, ha a hálózatba egy eddiginél nagyobb verziószámmal rendelkező kapcsoló kerül. Mivel egy kapcsoló alapesetben kiszolgáló, így az új, de nem helyes információk felülírják a korábbi VLAN adatokat minden kapcsolón.

Ennek a helyzetnek az elkerülésére beállítható a kapcsoló azonosítására szolgáló VTP jelszó. További megoldás jelent, ha mielőtt egy kiszolgáló módú kapcsolót már tartalmazó hálózathoz új kapcsolót adunk, megbizonyosodunk róla, hogy a kapcsoló ügyfél vagy transzparens módban van-e.



Három VTP üzenettípus létezik: összegző hirdetmény, részleges hirdetmény és hirdetménykérés.

Összegző hirdetmény

A Catalyst kapcsolók 5 másodpercenként vagy a VLAN adatbázis változásakor küldik összegző hirdetményeiket. Ezek tartalmazzák az aktuális VTP tartomány nevét és a konfiguráció verziószámát.

VLAN létrehozásakor, törlésekor vagy változtatásakor a kiszolgáló eggyel megnöveli a verziószámot, és elküld egy összegző hirdetményt.

Amikor egy kapcsoló összegző hirdetményt kap, összehasonlítja a benne szereplő VTP tartomány nevét a sajátjával. Egyezés esetén ellenőrzi a verziószámot is. Kisebb vagy megegyező érték esetén eldobja a keretet, ellenkező esetben viszont egy hirdetménykérést küld.

Részleges hirdetmény

Az összegző hirdetményt VLAN információkat tartalmazó részleges hirdetmény követi.

A részleges hirdetményekben találhatók az összegző hirdetményhez kapcsolódó új VLAN információk. Ha több VLAN létezik, akkor több részleges hirdetményre van szükség.

Hirdetménykérés

A Catalyst kapcsolók a VLAN információkat hirdetménykérésekkel kérdezik le. Erre akkor kerül sor, ha a kapcsolót törölték, a VTP tartomány neve megváltozott vagy a kapcsoló a sajátjánál nagyobb verziószámú VTP összegző hirdetményt kapott.

3.5.2 A VTP konfigurálása

A kapcsolók alapesetben kiszolgáló módban vannak. Amikor egy kiszolgáló módban levő kapcsoló az eddig érvényben lévőnél nagyobb verziószámú frissítést küld, az összes többi kapcsoló az új információnak megfelelően változtatja meg adatbázisát.

Új kapcsoló meglévő tartományhoz csatlakoztatásakor a következő lépéseket kell elvégezni:

1. lépés: VTP konfigurálása off-line módban (1-es verzió)
2. lépés: VTP konfiguráció ellenőrzése
3. lépés: Kapcsoló újraindítása

3.5.3 VLAN-ok az IP-telefónia és a vezeték nélküli hálózatok világában

A VLAN-ok létrehozásának alapvető célja a forgalom logikai csoportokra bontása. Egy VLAN forgalma nem befolyásolja egy másik VLAN forgalmát. A VLAN-környezet ideális a késleltetésre érzékeny forgalom, például hangátvitel esetén.

A szakadozott és rosszul hallható beszélgetések elkerülése érdekében a hangátvitel számára prioritást kell biztosítani az adatátvitellel szemben. Hangátvitelre szolgáló külön VLAN létrehozásával elkerülhető a kétfajta forgalom versengése a rendelkezésre álló sávszélességen.

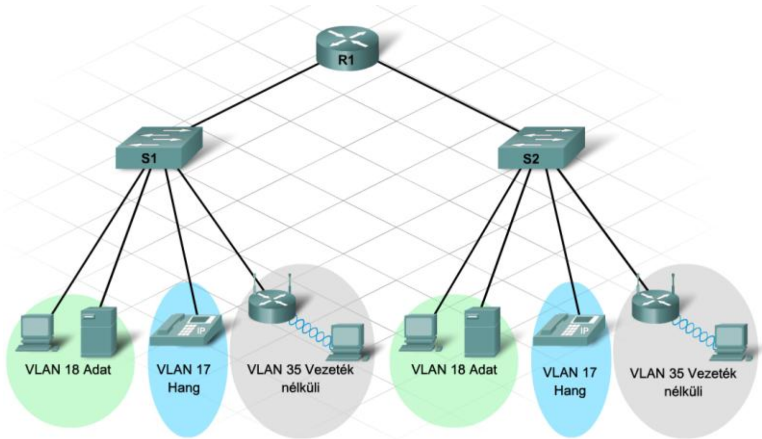
Egy IP-telefonnak általában 2 portja van, az egyik a hang-, a másik pedig az adatátvitel számára. A számítógéptől és az IP-telefontól kiinduló ill. oda beérkező csomagok a telefontól a kapcsolóig közös

fizikai összeköttetést, illetve ugyanazt a kapcsolóportot használják. A hangforgalom elválasztásához külön hangtovábbításra szolgáló VLAN-t érdemes létrehozni a kapcsolón.

Vezeték nélküli forgalom esetén szintén előnyökkel jár a VLAN-ok alkalmazása. A vezeték nélküli forgalom természeténél fogva nem biztonságos és a hekkerek kedvelt célpontja. VLAN-ok kialakításával néhány lehetséges probléma elkerülhető. A vezeték nélküli VLAN védelme miatt alkalmazott kötöttségek nincsenek hatással a szervezet többi VLAN-jára.

A legtöbb vezeték nélküli rendszernél a felhasználó biztonsági okokból a tűzfalon kívül csatlakozik a VLAN-hoz, és a vezeték nélküli hálózatból a belső hálózat eléréséhez azonosítania kell magát.

Számos szervezet biztosít vendég hozzáférést a vezeték nélküli hálózatához. A vendég hozzáférés ideiglenes jelleggel biztosít bárki számára olyan vezeték nélküli szolgáltatásokat, mint például web hozzáférés, elektronikus levelezés, ftp és SSH. A vendég felhasználók tartozhatnak a vezeték nélküli VLAN-ba vagy akár átkerülhetnek egy elkülönített vendég VLAN-ba is.



3.5.4 Bevált VLAN megoldások

Egy gondosan megtervezett és létrehozott VLAN struktúra védelmet nyújt, sávszélességet takarít meg, és lokalizálja a vállalati hálózat forgalmát. Mindezen tulajdonságokat együttesen kihasználva javítható a hálózat teljesítménye.

Néhány hasznos tanács VLAN-ok konfigurálásához vállalati hálózatokban:

- Kiszolgáló helyének megtervezése
- Nem használt portok letiltása
- A felügyeleti VLAN konfigurálása 1-estől eltérő VLAN-számmal
- VLAN trönkprotokoll használata
- VTP tartományok létrehozása
- Minden a meglévő hálózathoz csatlakozó új kapcsoló csatlakoztatás előtti újraindítása

A VLAN-ok nem nyújtanak minden problémára megoldást.

A nem megfelelően kialakított VLAN-ok feleslegesen bonyolulttá tehetik a hálózatot, ez inkonzisztens kapcsolatokhoz és a hálózat teljesítményének romlásához vezethet.

A VLAN-ok biztonsági okokból különítenek el bizonyos típusú forgalomtipusokat egymástól. A VLAN-ok közötti forgalomirányításhoz 3. rétegbeli eszközre van szükség, amely megnöveli a megvalósítás költségét és a hálózat késleltetését.

3.6 A fejezet összegzése

- A kapcsolók portjain a mikroszegmentáció külön ütközési tartományokat hoz létre.
- A 3. rétegbeli kapcsolás a speciális ASIC hardverben történik.
- A kapcsolók a tárol-és-továbbít vagy a közvetlen kapcsolás elve alapján továbbítják a forgalmat.
- A kapcsolókon alapvető biztonsági intézkedéseket kell elvégezni, hogy csak az arra jogosultak férjenek hozzá az eszközökhöz.
- A feszítőfa protokoll a kapcsolási hurkok elkerülése érdekében a redundáns összeköttetéseket letiltja.
- A feszítőfa csúcsán található a gyökérponti kapcsoló, amit a legalacsonyabb hídazonosító alapján választanak.
- A feszítőfa újraszámítása akár 50 másodpercig is tarthat, ami alatt a hálózat működése korlátozott.
- A gyors feszítőfa protokollt a konvergencia idő csökkentése érdekében fejlesztették ki.
- A VLAN olyan állomások gyűjteménye, melyek ugyanahhoz a helyi hálózathoz tartoznak annak ellenére, hogy fizikailag távol is elhelyezkedhetnek egymástól.
- Alapértelmezés szerint a VLAN 1 a felügyeleti VLAN.
- A keretcímkézés során kerül az Ethernet keretbe a VLAN azonosító, ami alapján egy kapcsoló azonosítja a forrás VLAN-t.
- Az IEEE 802.1Q nyílt keretcímkézési szabvány egy 4 bájtos címkét tesz az Ethernet keretbe.

- A hozzáférési port egy eszközt csatlakoztat a kapcsolóhoz, és egyetlen VLAN-ba tartozhat.
- A trönkport két kapcsolót vagy egy kapcsolót és egy forgalomirányítót köt össze, és alkalmas több VLAN-ból származó, címkével ellátott keretek továbbítására.
- A címke nélküli keretek a natív VLAN-ban kerülnek továbbításra.
- A különböző VLAN-ok közötti forgalom irányításához egy 3. rétegbeli eszközre van szükség.
- A forgalomirányító interfészén alinterfészek létrehozása biztosítja a több VLAN kezelését.
- A VLAN trönkprotokoll lehetővé teszi a vállalat VLAN adatbázisának központi ellenőrzését, elosztását és karbantartását.
- Egy kapcsoló lehet kiszolgáló, ügyfél vagy transzparens módban
- A legnagyobb verziószámmal rendelkező kiszolgáló VTP frissítéseket küld.
- A VLAN-ok alkalmasak az időzítésre érzékeny forgalom, mint például a hang továbbítására.
- A jól bevált módszerek, mint például a következetes VTP tartománynevek és verziószámok használata növeli a hálózat hatékonyságát.

4. Vállalati hálózatok címzése

4.1 IP-hálózatok hierarchikus címzési sémája

4.1.1 Egyszintű és hierarchikus hálózatok

A helyi hálózatban bekövetkező ütközések száma kapcsolók használatával csökkenthető. Egy teljesen kapcsolt hálózat általában egyetlen szórási tartományból áll. Ilyen egyszintű hálózatban minden eszköz ugyanabba a hálózatba tartozik, és minden szórási üzenetet megkap. Mindez kisebb hálózatok esetén elfogadható.

Sok állomás esetén egy egyszintű hálózat hatékonysága romlik. Ahogyan a kapcsolt hálózat állomásainak száma nő, úgy kell egyre több szórási üzenetet küldeni és fogadni. A szórási üzenetek sávszélességet foglalnak le, késleltetéseket és időtúllépéseket okoznak.

A nagyobb, egyszintű hálózatok problémájára megoldást nyújthat a VLAN-ok (virtuális helyi hálózatok) létrehozása. Ebben az esetben minden VLAN egy külön szórási tartomány.

Másik megoldás lehet forgalomirányítók használatával hierarchikus hálózat kialakítása.

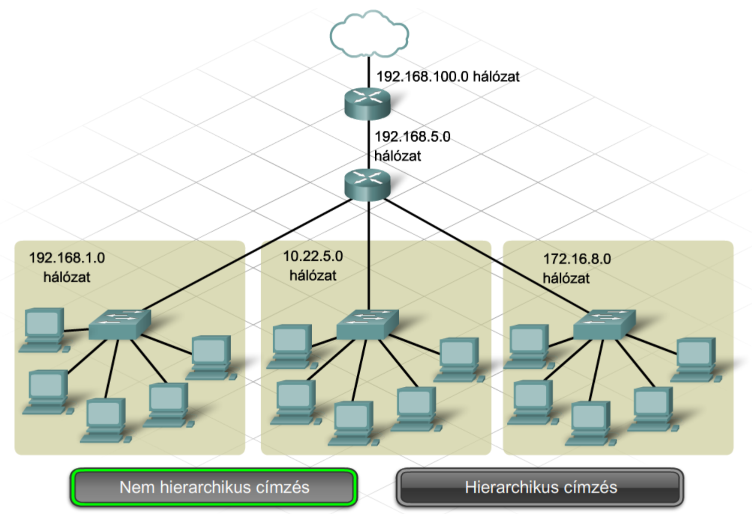
4.1.2 Hierarchikus hálózati címzés

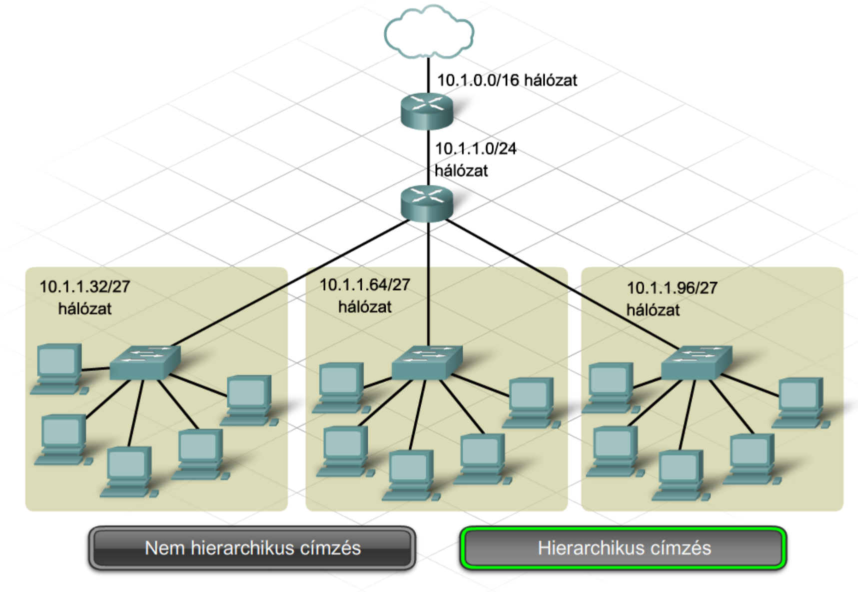
A vállalati hálózatok nagy kiterjedésűek és élhetnek a hierarchikus hálózattervezés és címzés előnyeivel. A hierarchikus címzés a hálózatot logikailag kisebb alhálózatokra osztja.

A hatékony hierarchikus címzési séma osztály alapú hálózati címzést használ a központi rétegben, majd fokozatosan egyre kisebb méretű alhálózatokat az elosztási és hozzáférési rétegben.

Hierarchikus hálózat hierarchikus címzés nélkül is működhet, de hatékonysága csökken, és néhány irányító protokoll tulajdonság, mint például az útvonalak összegzése nem megfelelően működik.

A földrajzilag különálló telephellyel rendelkező vállalati hálózatok esetében a hierarchikus tervezés és címzés egyszerűsíti a hálózat felügyeletét, a hibaelhárítást, és javitja a bővithetőséget és a forgalomirányítás hatékonyságát.





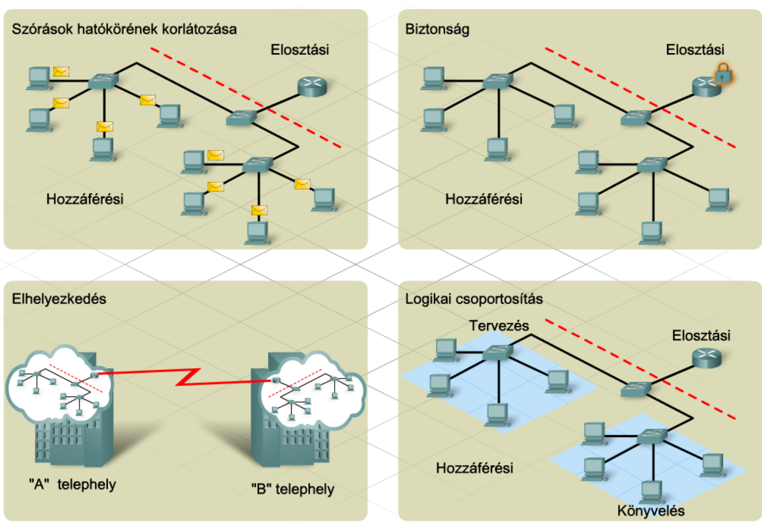
4.1.3 Hálózat felosztása alhálózatokra

hálózatok alhálózatokra bontásának számos oka lehet, köztük az alábbiak:

- Fizikai elhelyezkedés
- Logikai csoportosítás
- Biztonság
- Alkalmazási követelmények
- Szórások hatókörének korlátozása
- Hierarchikus tervezés

Ha egy szervezet például a 10.0.0.0 hálózatot használja, akkor alkalmazhatja a 10.X.Y.0 címzési sémát, ahol X egy földrajzi területet, Y pedig azon belül egy épületet vagy emeletet jelöl. Ez a címzés lehetővé teszi:

- 255 különböző földrajzi terület,
- területenként 255 épület,
- épületenként 254 állomás létrehozását.



4.2 A VLSM használata

4.2.1 Alhálózati maszk

A hierarchikus tervezéshez szükséges alhálózatok létrehozásához elengedhetetlen az alhálózati maszk fogalmának pontos ismerete és megértése.

Az alhálózati maszk azonositja az ugyanabba a hálózatba tartozó állomásokat. A maszk 32 bites, és az IP-cím hálózati és állomás bitjeit különbözteti meg egymástól. Felépítését tekintve 1-eseket majd 0-kat tartalmaz. Az 1-es bit a hálózati, a 0-ás bit pedig az állomás biteket azonosítja.

- Az A osztályú címek alapértelmezett alhálózati maszkja 255.0.0.0, vagy perjeles formában: /8.
- A B osztályú címek alapértelmezett alhálózati maszkja 255.255.0.0, azaz /16.
- A C osztályú címek alapértelmezett alhálózati maszkja 255.255.255.0, azaz /24.

A /x forma a cím hálózat azonositásra használt bitjeinek számát adja meg.

Egy vállalati hálózatban az alhálózati maszk hossza különböző lehet. Az egyes LAN szegmensekhez ugyanis gyakran eltérő számú állomás tartozik, és ilyenkor ugyanannak a maszknak a használata nem hatékony.

Pontozott decimális alhálózati maszk	Bináris alhálózati maszk	Perjeles forma	Állomásbitek száma	Megcímezhető állomások száma 2^n-2
255.0.0.0	11111111.00000000.00000000.00000000	/8	24	16777214
255.128.0.0	11111111.10000000.00000000.00000000	/9	23	8388606
255.192.0.0	11111111.11000000.00000000.00000000	/10	22	4194302
255.224.0.0	11111111.11100000.00000000.00000000	/11	21	2097150
255.240.0.0	11111111.11110000.00000000.00000000	/12	20	1048574
255.248.0.0	11111111.11111000.00000000.00000000	/13	19	524286
255.252.0.0	11111111.11111100.00000000.00000000	/14	18	262142
255.254.0.0	11111111.11111110.00000000.00000000	/15	17	131070
255.255.0.0	11111111.11111111.00000000.00000000	/16	16	65534
255.255.128.0	11111111.11111111.10000000.00000000	/17	15	32766
255.255.192.0	11111111.11111111.11000000.00000000	/18	14	16382
255.255.224.0	11111111.11111111.11100000.00000000	/19	13	8190
255.255.240.0	11111111.11111111.11110000.00000000	/20	12	4094
255.255.248.0	11111111.11111111.11111000.00000000	/21	11	2046
255.255.252.0	11111111.11111111.11111100.00000000	/22	10	1022
255.255.254.0	11111111.11111111.11111110.00000000	/23	9	510
255.255.255.0	11111111.11111111.11111111.00000000	/24	8	254
255.255.255.128	11111111.11111111.11111111.10000000	/25	7	126
255.255.255.192	11111111.11111111.11111111.11000000	/26	6	62
255.255.255.224	11111111.11111111.11111111.11100000	/27	5	30
255.255.255.240	11111111.11111111.11111111.11110000	/28	4	14
255.255.255.248	11111111.11111111.11111111.11111000	/29	3	6
255.255.255.252	11111111.11111111.11111111.11111100	/30	2	2

4.2.2 Alhálózat-számítás bináris formában

Amikor egy állomás kommunikációt kezdeményez egy másik állomással, akkor meghatározza a saját és a cél hálózati címét. Annak eldöntésére, hogy a két állomás ugyanahhoz a helyi hálózathoz csatlakozik-e, a küldő a saját alhálózati maszkját alkalmazza mind a saját, mind a célállomás IPv4 címére.

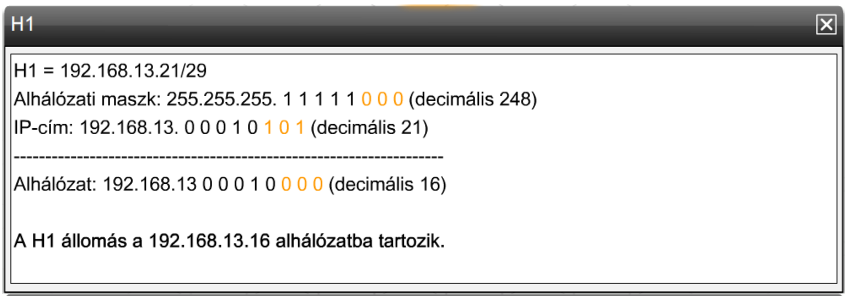
Az alhálózati maszk 32 bites és az IP-cím hálózati és állomás bitjeinek megkülönböztetésére szolgál. Felépítését tekintve 1-esek majd 0-ák sorozatából áll. Az 1-es bitek az IP-cím hálózatcímzésre szolgáló bitjeit, a 0-ás bitek pedig az állomáscímzésre használt biteket azonosítja. A küldő állomás a forrás- és a célcím hálózat-azonosító bitjeit hasonlítja össze. Amennyiben a két hálózatcím megegyezik, a csomag helyileg továbbítható, ellenkező esetben a csomagot az alapértelmezett átjárónak kell küldeni.

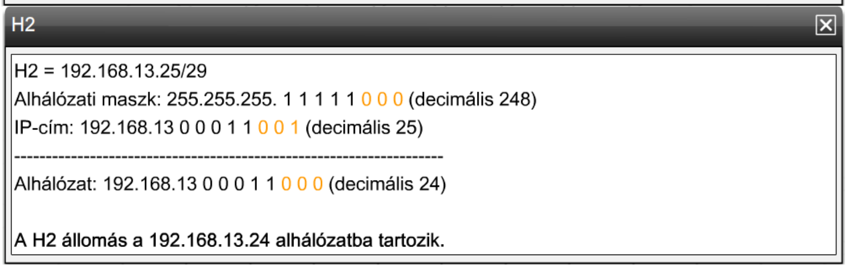
Tegyük fel, hogy a H1 állomás a 192.168.1.44 IP-címmel és a 255.255.255.0 alhálózati maszkkal üzenetet szeretne küldeni a H2 állomásnak, melynek IP-címe 192.168.1.66, alhálózati maszkja 255.255.255.0. Ebben az esetben mindkét állomás alapértelmezett maszkkal rendelkezik, azaz a hálózati bitek oktetthatáron (bájthatáron), mégpedig a harmadik oktettnél végződnek. Mivel mindkét állomás hálózati bitjei egyformán 192.168.1, így ugyanabban a hálózatban vannak.



Bár bájthatáron végződő alhálózati maszk esetén könnyű az IP-cím hálózati és állomás részének felismerése, maga a folyamat ugyanaz abban az esetben is, amikor a hálózati bitek nem oktetthatáron végződnek. Legyen például a H1 állomás IP-címe 192.168.13.21, alhálózati maszkja 255.255.255.248, azaz /29. Mindez azt jelenti, hogy a 32 bitből 29 bit a hálózatcim, vagyis a hálózati bitek az első három oktettet teljesen, a negyedik oktettet részben fedik le. Ebben az esetben a hálózat azonosítója 192.168.13.16.

Ha a 192.168.13.21/29 IP-című H1 állomás üzenetet szeretne küldeni a 192.168.13.25/29 IP-című H2 állomásnak, a hálózati bitek összehasonlítása szükséges annak eldöntésére, hogy a két állomás ugyanazon a helyi hálózaton található-e. Jelen esetben H1 hálózatazonosítója 192.168.13.16, H2 hálózatazonosítója pedig 192.168.13.24, így H1 és H2 nem ugyanahhoz a hálózathoz tartozik, ezért kommunikációjukhoz forgalomirányító szükséges.





4.2.3 Alapszintű alhálózat-készítés

Hierarchikus címzés esetén számos információ meghatározható csupán az IP-cím és az alhálózati maszk perjeles (/X) formájából. A 192.168.1.74/26 IP-cím például a következő információkat tartalmazza:

Decimális alhálózati maszk

- A /26 formának megfelelő alhálózati maszk a 255.255.255.192.

Létrehozott alhálózatok száma

- Az alapértelmezett /24 maszkból kiindulva 2 állomásbit lett átsorolva a hálózatcimzésre szolgáló bitekhez, e két bittel 4 alhálózat hozható létre (2^2 = 4).

Alhálózatonként megcímezhető állomások száma

- 6 állomásbit segítségével 62 állomás címezhető meg alhálózatonként (2^6 – 2 = 64 - 2 = 62).

Hálózati cím

- Az alhálózati maszk segítségével meghatározhatók a hálózati bitek, és így a hálózati cím is. A példában ez 192.168.1.64.

Első használható állomáscím

- Egy állomás IP-címében nem lehet minden állomásbit 0, mivel az az alhálózat hálózati címe. Így az első használható állomáscím a .64-es alhálózatban a .65

Üzenetszórási cím

- Egy állomás IP-címében nem lehet minden állomásbit 1-es, mivel az az alhálózat üzenetszórási címe. Ebben az esetben az üzenetszórási cím .127, a következő alhálózat hálózati címe pedig .128.

Címzési séma: Példa 4 hálózatra

Alhálózat	Hálózati cím	Állomáscím tartomány	Üzenetszórási cím
0	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 - 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129- 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 - 192.168.1.254	192.168.1.255

4.2.4 Változó hosszúságú alhálózati maszk (VLSM)

Az alapszintű alhálózat-készítés kisebb hálózatok esetén megfelelő, de nem nyújt elegendő rugalmasságot nagyobb vállalati hálózatokban.

A változó hosszúságú alhálózati maszk (VLSM – Variable Length Subnet Mask) a címtér hatékony alkalmazását, és a hierarchikus IP-címzésnek köszönhetően az útvonalösszegzés kihasználását teszi lehetővé. Az útvonalösszegzés (összevonás) csökkenti az irányítótáblák méretét a hozzáférési és központi réteg forgalomirányítóiban. A kisebb irányítótáblában való keresés kevesebb CPU időt igényel.

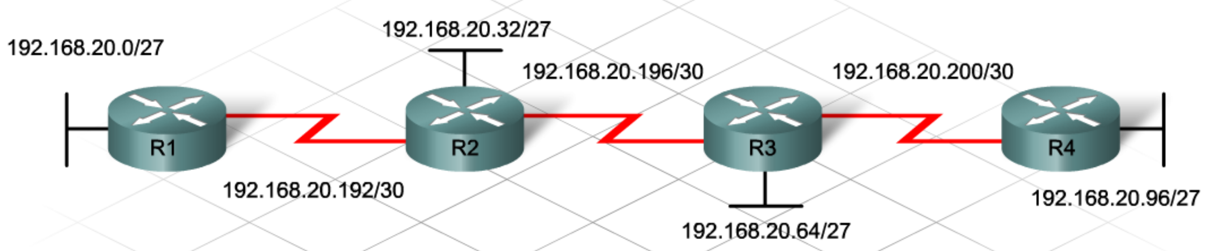
A VLSM az alhálózatok alhálózatokra bontásának elve. Kezdetben a címzés hatékonyságának maximalizálására fejlesztették ki, később a privát címek megjelenésével elsődleges előnye a szervezhetőség és az útvonalösszegzés lett.

Nem minden irányító protokoll támogatja a VLSM használatát. Az osztály alapú irányító protokollok, mint például a RIPv1, útvonalfrissítéseikben nem tartalmazzák az alhálózati maszkot. Adott alhálózati maszkkal rendelkező interfész esetén a forgalomirányító feltételezi, hogy minden ugyanebbe az osztályba tarozó csomag ugyanilyen maszkkal rendelkezik.

Az osztály nélküli irányító protokollok támogatják a VLSM használatát, mivel minden útvonalfrissítésben elküldik az alhálózati maszkot. Osztály nélküli irányító protokoll például a RIPv2, az EIGRP és az OSPF.

A VLSM előnyei:

- Címtér hatékony kihasználása
- Eltérő alhálózati maszk hossz használata
- Címblokkok kisebb egységekre bontása
- Útvonalösszegzés
- Rugalmasabb hálózattervezés
- Hierarchikus vállalati hálózatok támogatása



192.168.20.0 alhálózatai	
Alhálózat azonosító	Alhálózati cím
0. alhálózat	192.168.20.0/27
1. alhálózat	192.168.20.32/27
2. alhálózat	192.168.20.64/27
3. alhálózat	192.168.20.96/27
4. alhálózat	192.168.20.128/27
5. alhálózat	192.168.20.160/27
6. alhálózat	192.168.20.192/27
7. alhálózat	192.168.20.224/27

A 192.168.20.192 alhálózat alhálózatai	
Alhálózat azonosító	Alhálózati cím
0. alhálózat	192.168.20.192/30
1. alhálózat	192.168.20.196/30
2. alhálózat	192.168.20.200/30
3. alhálózat	192.168.20.204/30
4. alhálózat	192.168.20.208/30
5. alhálózat	192.168.20.212/30
6. alhálózat	192.168.20.216/30
7. alhálózat	192.168.20.220/30

A VLSM lehetővé teszi az akár alhálózatonként különböző alhálózati maszkok használatát. Egy hálózati cím alhálózatokra bontását követő minden további felbontás újabb alhálózatokat (al-alhálózatokat) hoz létre.

A 10.0.0.0/8 hálózatot például egy /16-os alhálózati maszk 256 alhálózatra bontja, melyek mindegyikében 16382 állomás címezhető.

10.0.0.0/16

10.1.0.0/16

10.2.0.0/16 - 10.255.0.0/16

A /24 alhálózati maszkot alkalmazva bármely /16 alhálózatra, például, a 10.1.0.0/16-ra, 256 további alhálózat jön létre. Az így kapott új alhálózatok mindegyike 254 állomás címzésére alkalmasak.

10.1.1.0/24

10.1.2.0/24

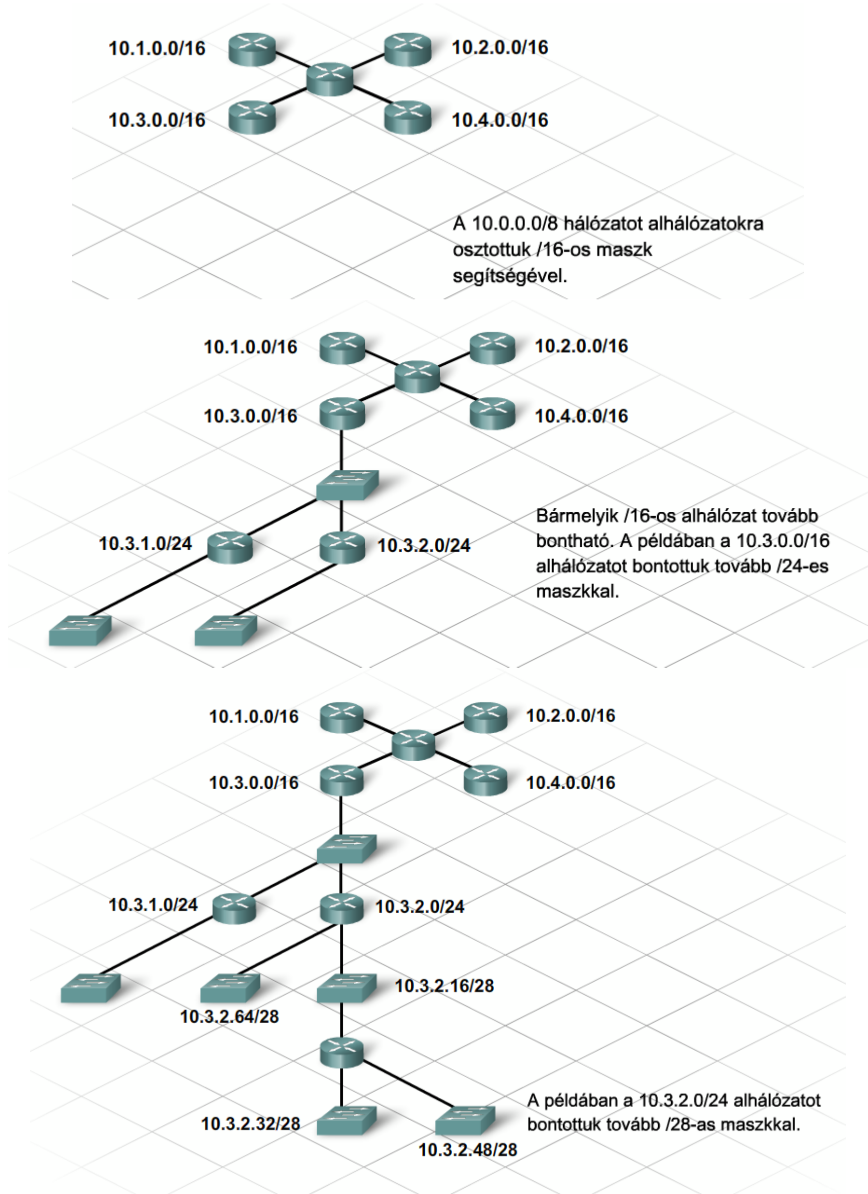
10.1.3.0/24 - 10.1.255.0/24

Bármely /24 alhálózatra alkalmazva a /28 alhálózati maszkot, 16 újabb alhálózat jön létre (például 10.1.3.0/28). Az így kapott új alhálózatok mindgyike 14 állomás címzésére alkalmasak.

10.1.3.0/28

10.1.3.16/28

10.1.3.32/28 – 10.1.3.240/28

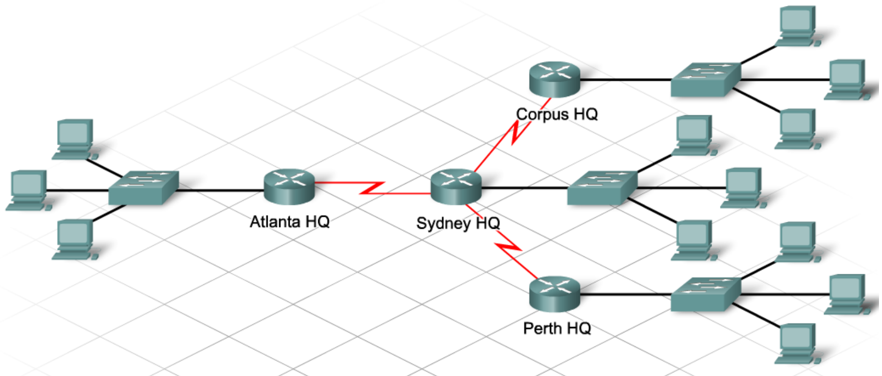


4.2.5 VLSM címzés megvalósítása

Egy IP-címzési séma létrehozása VLSM használatával gyakorlást és tervezést igényel. Gyakorlásképpen képzeljünk el egy olyan összetett hálózatot, amelyben a következő elvárások jelentkeznek:

- Atlanta HQ = 58 állomáscím
- Perth HQ = 26 állomáscím
- Sydney HQ = 10 állomáscím
- Corpus HQ = 10 állomáscím
- WAN összeköttetések = 2 állomáscím (összeköttetésenként)

A legnagyobb hálózat 58 állomásának címzéséhez /26-os alhálózat szükséges. Az egyszerű alhálózati séma használata nem csak pazarló, de mindösszesen 4 alhálózat létrehozását teszi lehetővé, ami nem elegendő a szükséges 7 LAN/WAN szegmens címzéséhez. A megoldást a VLSM címzés nyújtja.



Központok	Követelmények	Kihasználatlan címek
Atlanta HQ	58 állomáscím	4 cím
Perth HQ	26 állomáscím	36 cím
Sydney HQ	10 állomáscím	52 cím
Corpus HQ	10 állomáscím	52 cím
WAN-összeköttetések	2 állomáscím (összeköttetésenként)	60 cím

VLSM alhálózati séma kialakításánál az alhálózati követelmények megtervezésekor mindig figyelembe kell venni az állomások számának esetleges növekedését.

Név - szükséges állomáscím	Alhálózati cím	Címtartomány	Üzenetszórási cím	Hálózat/prefix
AtlantaHQ-58				
PerthHQ-28				
SydneyHQ-10				
CorpusHQ-10				
WAN1-2				
WAN2-2				
WAN3-2				

Hálózati követelmények felsorolása a legnagyobb hálózattól a legkisebbig.

Név - szükséges állomáscím	Alhálózati cím	Címtartomány	Üzenetszórási cím	Hálózat/prefix
AtlantaHQ-58	192.168.15.0	.1 - .62	.63	192.168.15.0/26
PerthHQ-28				
SydneyHQ-10				
CorpusHQ-10				
WAN1-2				
WAN2-2				
WAN3-2				

A legnagyobb AtlantaHQ LAN 58 állomáscímet igényel.
2 bit elvételével /26-os maszk használható.
Az így létrejövő 4 alhálózat: 192.168.15.0,192.168.15.64, 192.168.15.128, 192.168.15.192.
Az AtlantaHQ címzéséhez használjuk a 192.168.15.0/26 alhálózatot.

Név - szükséges állomáscím	Alhálózati cím	Címtartomány	Üzenetszórási cím	Hálózat/prefix
AtlantaHQ-58	192.168.15.0	.1 - .62	.63	192.168.15.0/26
PerthHQ-28	192.168.15.64	.65 - .94	.95	192.168.15.64/27
SydneyHQ-10				
CorpusHQ-10				
WAN1-2				
WAN2-2				
WAN3-2				

A PerthHQ LAN 28 állomáscímet igényel.
Használjuk a következő, 192.168.15.64/26 hálózatot.
További egy bit elvételével /27-es címblokk alakítható ki.
Az így létrejövő 2 alhálózat: 192.168.15.64, 192.168.15.96.
A PerthHQ címzéséhez használjuk a 192.168.15.64/27 alhálózatot.

Név - szükséges állomáscím	Alhálózati cím	Címtartomány	Üzenetszórási cím	Hálózat/prefix
AtlantaHQ-58	192.168.15.0	.1 - .62	.63	192.168.15.0/26
PerthHQ-28	192.168.15.64	.65 - .94	.95	192.168.15.64/27
SydneyHQ-10	192.168.15.96	.97 - .110	.111	192.168.15.96/28
CorpusHQ-10	192.168.15.112	.113 - .126	.127	192.168.15.112/28
WAN1-2				
WAN2-2				
WAN3-2				

A SydneyHQ és CorpusHQ LAN-ok 10 állomáscímet igényelnek.
Használjuk a következő, 192.168.15.96/27 hálózatot.
További bit elvételével a maszk /28-asra bővíthető.
Az így létrejövő 2 alhálózat: 192.168.15.96, 192.168.15.112.
Az egyiket használjuk a SydneyHQ, a másikat a CorpusHQ hálózat címzéséhez.

Név - szükséges állomáscím	Alhálózati cím	Címtartomány	Üzenetszórási cím	Hálózat/prefix
AtlantaHQ-58	192.168.15.0	.1 - .62	.63	192.168.15.0/26
PerthHQ-28	192.168.15.64	.65 - .94	.95	192.168.15.64/27
SydneyHQ-10	192.168.15.96	.97 - .110	.111	192.168.15.96/28
CorpusHQ-10	192.168.15.112	.113 - .126	.127	192.168.15.112/28
WAN1-2	192.168.15.128	.129 - .130	.131	192.168.15.128/30
WAN2-2	192.168.15.132	.133 - .134	.135	192.168.15.132/30
WAN3-2	192.168.15.136	.137 - .138	.139	192.168.15.136/30

A három pont-pont WAN-összeköttetés mindegyikéhez két cím szükséges.
Használjuk a következő, 192.168.15.128/28 alhálózatot.
További 2 bit elvételével /30-as maszkot kapunk.
Az így létrejövő alhálózatok: 192.168.15.128, 192.168.15.132, 192.168.15.136.
Használjuk mind a három alhálózatot a WAN-összeköttetésekhez.

Számos címzési rendszer kialakítását támogató eszköz létezik.

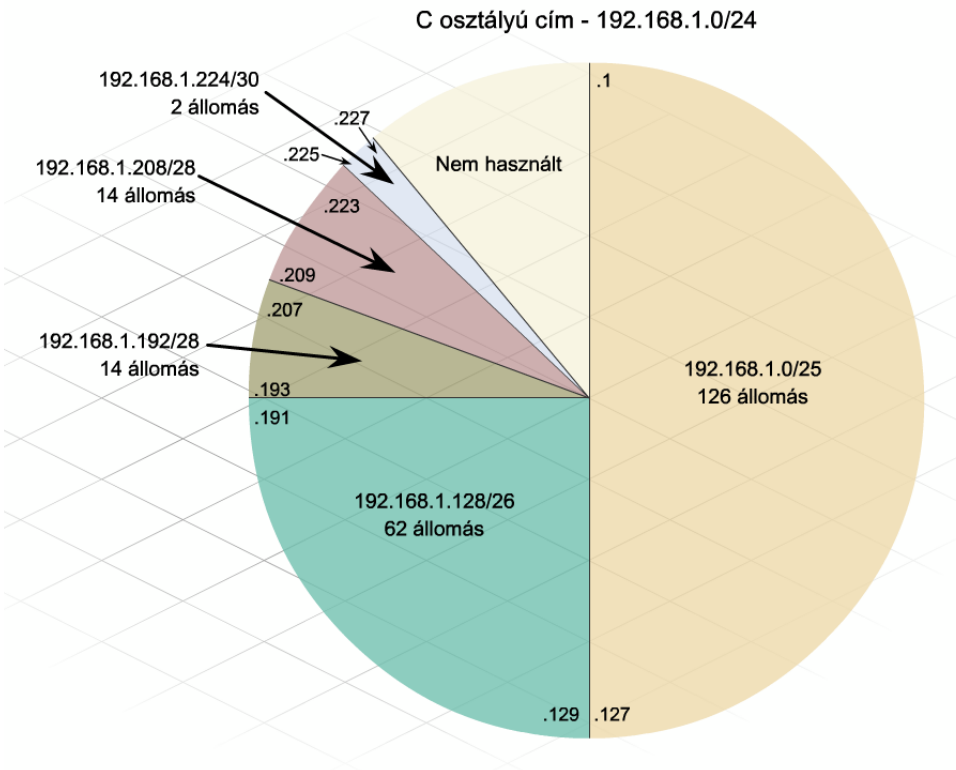
VLSM diagram

Az egyik ilyen módszer VLSM diagram segítségével azonosítja a még felhasználható és a már kiosztott címblokkokat.

VLSM kördiagram

Egy másik megoldás egy kördiagram segítségével, a teljes kört kisebb körcikkekre osztva ábrázolja az alhálózatokat.

Ezek az eljárások megakadályozzák a már lefoglalt címek újbóli kiosztását, és segítenek az átfedő címtartományok kialakításának elkerülésében.



4.3 Az osztály nélküli forgalomirányítás és a CIDR alkalmazása

4.3.1 Osztály alapú és osztály nélküli forgalomirányítás

A VLSM és hasonló módszerek alkalmazásával az osztály alapú IPv4 címzési rendszer kiterjeszthető osztály nélküli rendszerré. Az osztály nélküli címzés az internet exponenciális növekedését tette lehetővé.

Az osztály alapú címzés az IP-címek három alap osztályát és a hozzájuk tartozó alapértelmezett alhálózati maszkokat határozza meg:

- A osztály (255.0.0.0 vagy /8)
- B osztály (255.255.0.0 vagy /16)
- C osztály (255.255.255.0 vagy /24)

Egy vállalat A osztályú hálózati címtartomány használata esetén több mint 16 millió, B osztály esetén több mint 65.000, míg C osztály esetén mindösszesen 254 állomáscímmel rendelkezik. Amióta a felhasználható A és B osztályú címek száma korlátozott, sok vállalat több C osztályú cím beszerzésével biztosítja a hálózat követelményeinek megfelelő számú címet.

Ennek következményeként a C osztályú címtér kimerülése az eredetileg tervezettnél lényegesen gyorsabban megtörtént.

	1. oktett	2. oktett	3. oktett	4. oktett	Alhálózati maszk
A osztály	Hálózat	Állomás	Állomás	Állomás	255.0.0.0 vagy /8
B osztály	Hálózat	Hálózat	Állomás	Állomás	255.255.0.0 vagy /16
C osztály	Hálózat	Hálózat	Hálózat	Állomás	255.255.255.0 vagy /24

Címosztály	Első oktett értéktartománya	Létrehozható hálózatok száma	Állomások száma hálózatonként
A osztály	0 - 127	128 (2 foglalt)	16 777214
B osztály	128 - 191	16348	65534
C osztály	192 - 223	2 097152	254

Osztály alapú IP-címek esetén az első oktett, azon belül is az első három bit értéke határozza meg, hogy a hálózat A, B vagy C osztályú. Minden fő hálózathoz egy alapértelmezett maszk tartozik, melyek rendre 255.0.0.0, 255.255.0.0 vagy 255.255.255.0.

Az **osztály alapú** irányító protokollok, mint például a RIPv1, útvonalfrissítései nem tartalmazzák az alhálózati maszkot, így a fogadó forgalomirányítók ezeket feltételezések alapján határozzák meg.

Osztály alapú irányító protokoll esetén, ha egy forgalomirányító frissítést küld egy alhálózatokra bontott hálózatról, például a 172.16.1.0/24-ről, egy olyan forgalomirányítónak, melynek interfésze a frissítésben szereplő főhálózathoz tartozik, például a 172.16.2.0/24-hez, akkor a következő történik:

- A küldő forgalomirányító a teljes hálózati címet hirdeti alhálózati maszk nélkül, ami ebben az esetben 172.6.1.0.
- A fogadó forgalomirányító a 172.16.2.0 interfészének megfelelő alhálózati maszkot alkalmazza a hirdetett hálózatra, azaz a példában a 255.255.255.0 maszkot a 172.16.1.0 hálózatra.

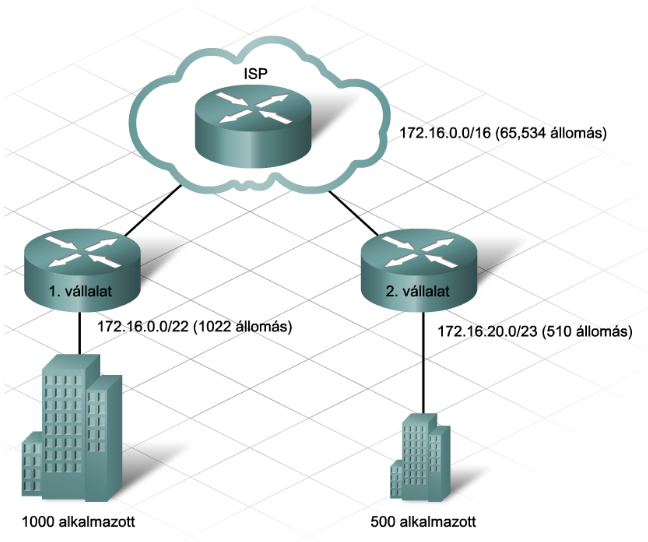
Ha a forgalomirányító frissítést küld egy alhálózatokra bontott hálózatról, például a 172.16.1.0/24-ről, egy olyan forgalomirányítónak, melynek interfésze nem a frissítésben szereplő fő hálózathoz tartozik, hanem például a 192.168.1.0/24-hez, akkor a következő történik:

- A küldő forgalomirányító nem az alhálózati, csak a fő osztály alapú hálózati címet hirdeti, ami ebben az esetben 172.16.0.0.
- A fogadó forgalomirányító alkalmazza erre a hálózatra az alapértelmezett alhálózati maszkot, ami B osztály esetén 255.255.0.0.

Az IPv4 címek gyors kimerülésére reagálva fejlesztette ki az IETF az osztály nélküli forgalomirányítást (Classless Inter-Domain Routing - CIDR). A CIDR az IPv4 címtér hatékonyabb felhasználását teszi lehetővé, alkalmas hálózati címek összegzésére, és így az irányítótáblák méretének csökkentésére.

A CIDR használata osztály nélküli irányító protokollt igényel, például RIPv2-t, EIGRP-t vagy statikus forgalomirányítást. CIDR kompatibilis forgalomirányítók esetén a címosztályoknak nincs jelentősége. Az alhálózati maszk meghatározza a cím hálózati részét, amelyet hálózati előtagnak (network prefix) vagy előtag hossznak is neveznek. A cím osztálya ebben az esetben már nem határozza meg a hálózati címet.

Az internetszolgáltatók az ügyfelek néhány állomástól akár több száz vagy több ezer állomásig terjedő igényei szerint IP-címek megfelelő csoportját rendelik hozzá egy-egy ügyfélhálózathoz. CIDR és VLSM esetén már nem csak a /8-as, a /16-os vagy a /24-es előtag hosszt használhatják.



A VLSM-et és a CIDR-et támogató osztály nélküli irányító protokollok közé tartozó belső átjáró protokollok (IGP) a RIPv2, az EIGRP, az OSPF és az IS-IS. Az internetszolgáltatók külső átjáró protokollokat (EGP) is használnak. Példaként a határátjáró-protokollt (BGP – Border Gateway Protocol) említhető.

Az osztály alapú és osztály nélküli irányító protokollok közötti különbség lényege, hogy az osztály nélküli protokollok útvonal-frissítései a hálózati címeket a hozzájuk tartozó alhálózati maszkkal együtt hirdetik. Osztály nélküli irányító protokoll használata akkor elengedhetetlen, ha a maszk az első oktett értéke alapján nem határozható meg helyesen vagy egyértelműen.

Amikor egy forgalomirányító osztály nélküli protokollt használva útvonalfrissítést küld, például a 172.16.1.0 hálózatról, egy olyan fogalomirányítónak, amelynek hirdetést fogadó interfésze a frissítésben hirdetett fő hálózathoz tartozik, például a 172.16.2.0/24 hálózat része, akkor a következő történik:

- A küldő forgalomirányító minden alhálózatát alhálózati maszkkal együtt hirdeti.

Amikor egy forgalomirányító például a 172.16.1.0 hálózatról küld útvonalfrissítést egy olyan fogalomirányítónak, melynek hirdetést fogadó interfésze nem csatlakozik a frissítésben hirdetett fő hálózathoz, ehelyett például 192.168.1.0/24-hez tartozik, akkor a következő történik:

- A küldő forgalomirányító alapesetben minden alhálózatot összevon, és az osztály alapú fő hálózatot hirdeti az összevont alhálózati maszkkal együtt. Ezt a folyamatot nevezik hálózat határon történő útvonalösszegzésnek. A legtöbb osztály nélküli protokoll alapértelmezetten engedélyezi a hálózathatáron történő automatikus útvonalösszegzést, de lehetőség van ennek letiltására is.
- Letiltás esetén a küldő forgalomirányító minden alhálózatát alhálózati maszkkal együtt hirdeti.

4.3.2 CIDR és útvonalösszegzés

Az internet gyors bővülésének következtében a világ különböző hálózataihoz vezető útvonalak száma nagymértékben növekedett. A VLSM címzés lehetővé teszi az útvonalak összegzését, és így a hirdetett útvonalak számának csökkentését.

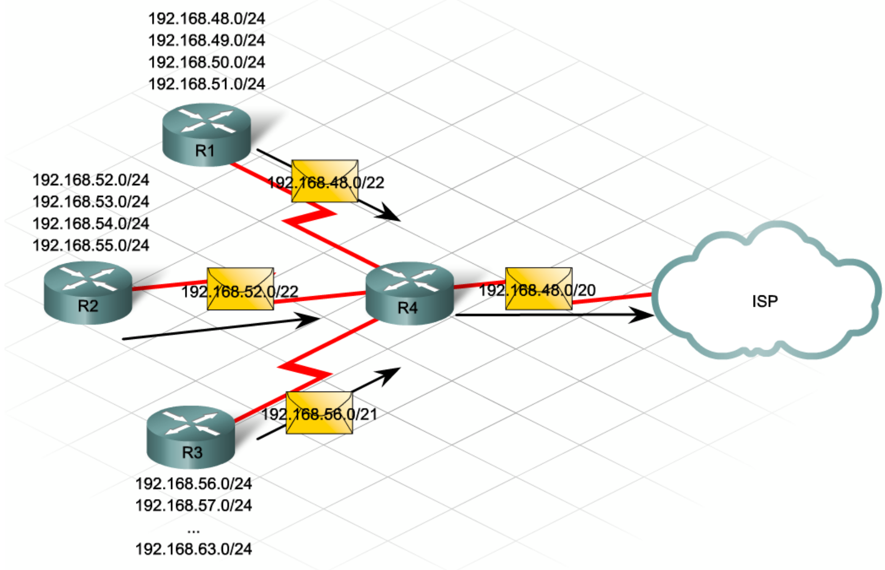
Az útvonalösszegzés az összefüggő hálózat- és alhálózatcimeket a hálózat határán levő határ-forgalomirányítón egyetlen összevont hálózatcímmel helyettesiti.

Az összegzés csökkenti az útvonalfrissítések gyakoriságát és az irányítótábla-bejegyzések számát. Javítja az útvonalfrissítések sávszélesség-kihasználását és gyorsítja az irányítótáblában való keresést.

Az útvonalösszegzés és a szuperhálózattá alakitás (supernetting) jelentése megegyezik. A szuperhálózattá alakitás az alhálózatokra bontás ellentéte, több kisebb összefüggő hálózat összevonása.

Ha a hálózati bitek száma nagyobb az osztály alapon értelmezett értéknél, mint például 172.16.3.0/26 esetén, akkor alhálózatról beszélünk. B osztályú cím esetén minden /16-osnál nagyobb előtag hossz alhálózatot jelöl.

Ha a hálózati bitek száma kisebb az osztály alapértelmezett értékénél, mint például 172.16.3.0/14 esetén, akkor szuperhálózatról beszélünk. B osztályú cím esetén minden /16-osnál kisebb előtag hossz szuperhálózatot jelöl.

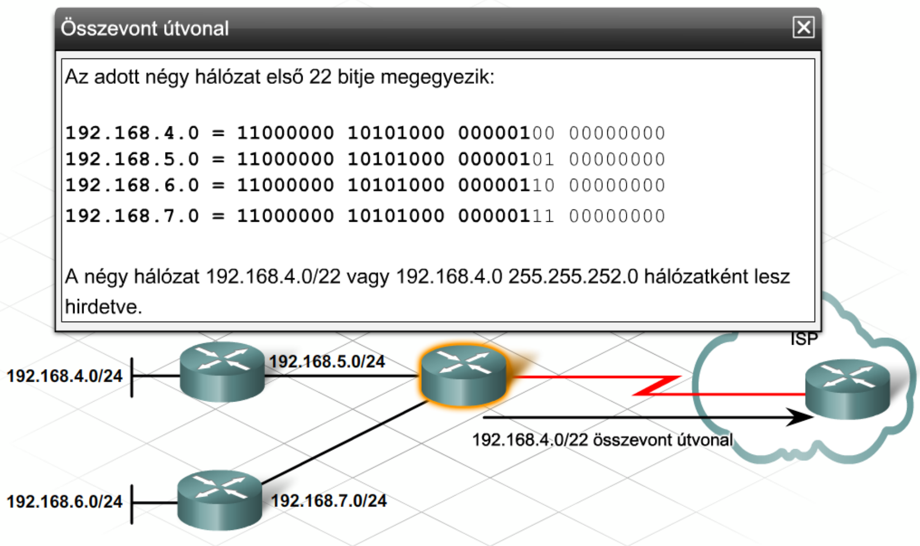


Útvonal-összevonási példa

Egy határ-forgalomirányító általában a vállalat minden ismert hálózatát hirdeti az internetszolgáltató felé. Ha például nyolc különböző hálózat van, akkor elképzelhető, hogy mind a nyolcat hirdetni fogja. Ha minden vállalat ugyanígy tenne, akkor az internetszolgáltató irányítótáblája hatalmasra nőne.

Útvonalösszegzéskor a forgalomirányító az összefüggő hálózatokat csoportosítja, és egyetlen nagy hálózatként hirdeti őket. A fenti megoldáshoz hasonló példa, amikor egy vállalat központi irodájához csak néhány központi szám tartozik a telefonkönyvben annak ellenére, hogy az egyes munkatársak mellékei közvetlenül is hívhatók.

Hierarchikus címzési rendszer esetén könnyebben elvégezhetők az útvonalösszegzések. Vállalaton belül olyan hálózatcímeket osszunk ki, amelyek CIDR használatával csoportosíthatók.



4.3.3 Az útvonalösszegzés meghatározása

Az összegzett útvonal meghatározásához az érintett hálózatcimeket egyetlen címmé kell összevonni, ami három lépésben történik:

1. lépés

Írjuk fel az érintett hálózatcímeket bináris formában.

2. lépés:

Az összegezett útvonal maszkjának megadásához határozzuk meg az összevonni kivánt hálózatcímekben a balról megegyező bitek számát. Ez a szám lesz az összegzett útvonal hálózati előtagja vagy alhálózati maszkja, például /14 vagy 255.252.0.0.

3. lépés:

Az összegzett hálózaticím meghatározásához az egyező biteket egészítsük ki 32 bites hosszúságra 0 bitértékekkel. (A nem megegyező biteket 0 bitekkel helyettesítjük.) Gyorsabb megoldáshoz vezet, ha a hálózatok között megkeressük a legkisebb hálózati címmel rendelkezőt.

Nem hierarchikus címzés esetén nem feltétlenül lehetséges az útvonalak összegzése. Ha a hálózati címekben balról jobbra összehasonlítva nincsenek megegyező bitek, akkor összefogott maszk nem határozható meg.



4.3.4 Nem összefüggő alhálózatok

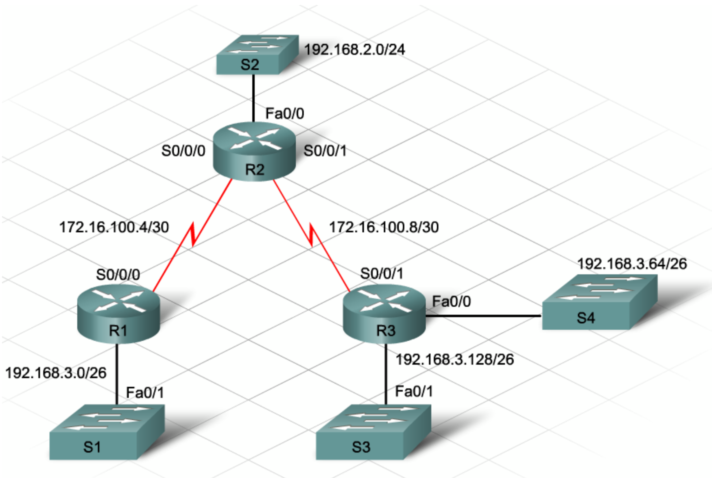
Az útvonal-összegzéseket vagy a rendszergazda maga konfigurálja, vagy az egyes irányító protokollok (például a RIPv1, a RIPv2 vagy az EIGRP) automatikusan teszik ezt meg. Fontos az összegzések felügyelete, hogy a forgalomirányítók félrevezető hálózati hirdetéseket ne küldjenek ki.

Tegyük fel, hogy három forgalomirányító az Ethernet interfészein a C osztályú 192.168.3.0 hálózat alhálózatait használja. A forgalomirányítók egymáshoz soros interfészeiken keresztül kapcsolódnak, és ezek egy másik, például a 172.16.100.0/24 fő hálózathoz tartoznak. Osztály alapú protokoll esetén mindegyik forgalomirányító a C osztályú főhálózatot hirdeti hálózati maszk nélkül. Ennek

eredményeként a közbülső forgalomirányító ugyanarról a hálózatról két különböző irányból is kap hirdetményt. Ebben az esetben beszélünk nem összefüggő (nem folytonos) hálózatról.

A nem összefüggő hálózatok megbízhatatlan. nem optimális forgalomirányítást eredményeznek. Ennek elkerülése érdekében a rendszergazda a következőket teheti:

- Lehetőség szerint módosítja a címzési sémát.
- Osztály nélküli irányító protokollt használ, például RIPv2-t vagy OSPF-et.
- Letiltja az automatikus összegzést.
- Manuálisan végzi el az útvonalösszegzést az osztály határon.



Körültekintő tervezést követően is előfordulhat, hogy a hálózatban nem összefüggő alhálózatok vannak. A következő forgalmi és forgalomirányítási példák segítenek ezeknek a helyzeteknek a felismerésében:

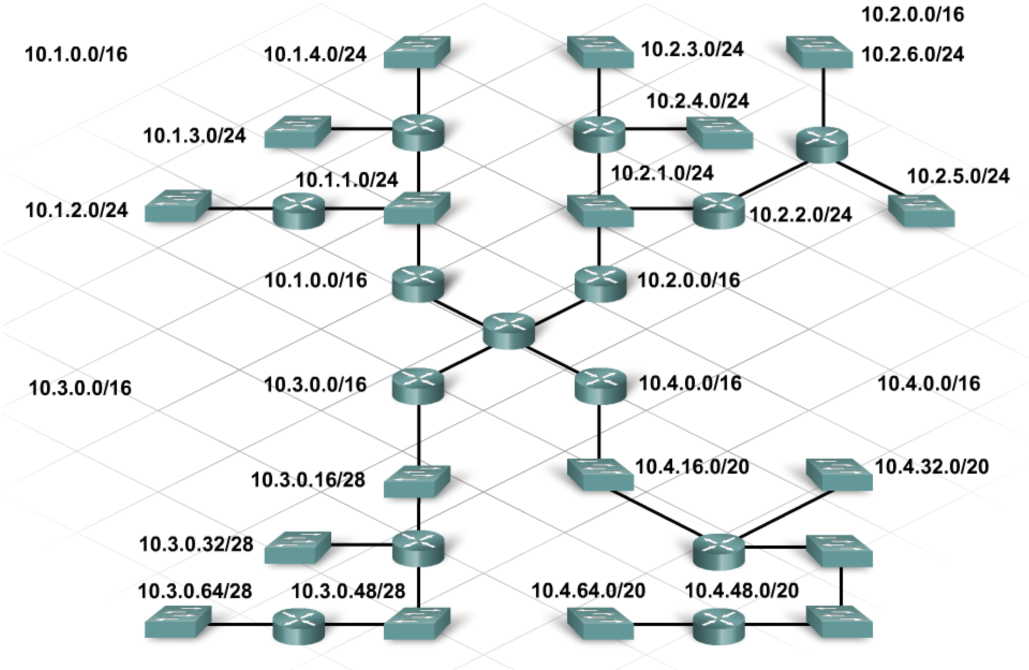
- Egy forgalomirányító nem ismer útvonalat egy másik forgalomirányítóhoz kapcsolódó LAN felé, pedig a hálózat hirdetését konfigurálták.
- Közbülső forgalomirányító két azonos költségű útvonalat ismer a fő hálózat felé annak ellenére, hogy az alhálózatok eltérő hálózati szegmensen találhatók.
- Közbülső forgalomirányító terheléselosztást végez a fő hálózat valamelyik alhálózata felé tartó forgalom esetében.
- A forgalomirányító feltételezhetően csak a forgalom felét kapja meg.

4.3.5 Alhálózatok létrehozásakor és címzésénél használt bevált módszerek

A hierarchikus hálózat létrehozásához nélkülözhetetlen egy helyesen megtervezett VLSM címzési rendszer. VLSM címzés kialakításakor kövessük a következő alapelveket:

- VLSM címzést és nem összefüggő alhálózatokat támogató, minél újabb irányító protokollokat alkalmazzunk.
- Szükség esetén az automatikus útvonalösszegzést tiltsuk le.
- A legfrissebb, nullás alhálózat használatát támogató IOS-t használjuk.
- Egy hálózaton belül a privát címtartományok keveredését kerüljük el.
- Lehetőség szerint a nem összefüggő alhálózatokat szüntessük meg.
- A címzés hatékonysága érdekében VLSM-t használjunk.

- Hierarchikus hálózattervezés és összefüggő címzési séma használatával az útvonalösszegzést tervezzük meg.
- Útvonalösszegzést használjunk a hálózat határain.
- WAN összeköttetésekhez /30-as alhálózatokat rendeljünk.
- A létrehozható alhálózatok és állomások számának tervezésekor a hálózat jövőbeni növekedését vegyük figyelembe.



4.4 NAT és PAT használata

4.4.1 Privát IP-címtér

A VLSM és a CIDR mellett a privát címzés és a hálózati címfordítás (NAT) használata tovább növelte az IPv4 címtér bővíthetőségét.

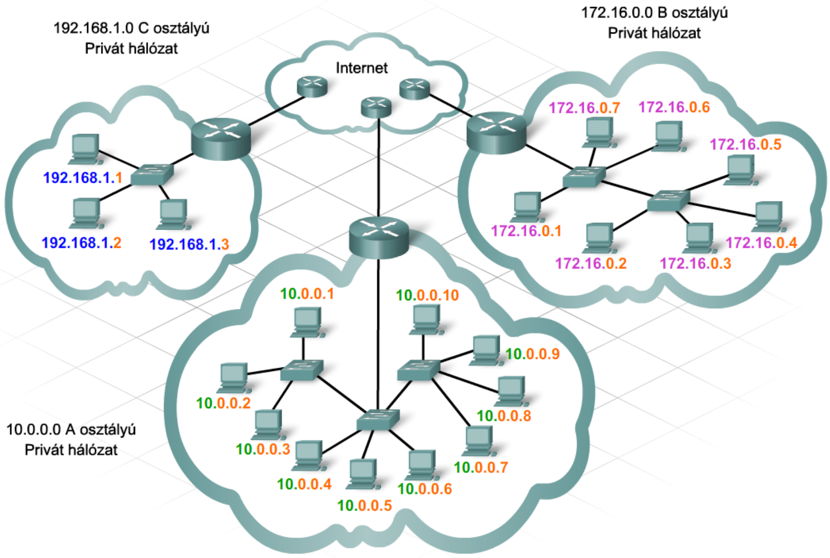
Privát címeket bárki alkalmazhat saját vállalati hálózatában, mivel ezek a címek csak a belső hálózatban irányíthatók, az interneten soha nem jelennek meg.

A privát címteret az RFC1918 definiálja.

- A osztály: 10.0.0.0 - 10.255.255.255
- B osztály: 172.16.0.0 - 172.31.255.255
- C osztály: 192.168.0.0 - 192.168.255.255

A privát címek használatának előnyei:

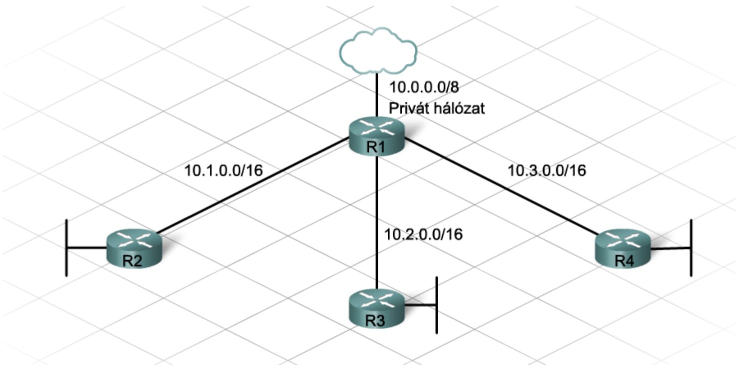
- Csökkenti az összes állomás nyilvános IP-címének beszerzésével járó magas költségeket.
- Lehetővé teszi, hogy több ezer belső alkalmazott használjon néhány nyilvános címet.
- Biztonságot nyújt azzal, hogy más hálózatok és szervezetek nem látják a belső címeket.



Belső hálózat privát címzési rendszerének kialakításakor alkalmazzuk a VLSM-nél használt hierarchikus tervezési elveket.

Bár a privát címek az interneten keresztül nem kerülnek továbbításra, a belső hálózatban gyakran kell őket irányítani. Mivel a nem összefüggő alhálózatok esetében felmerülő problémák előfordulhatnak privát címek használatakor is, így a címzési rendszer kialakítása gondos tervezést igényel.

Győződjünk meg arról, hogy a címek a VLSM-elveknek megfelelően, helyesen lettek kiosztva. A hatékony címösszegzés érdekében használjunk érvényes címhatárokat és hierarchikus IP-címzést.



4.4.2 NAT a vállalati hálózat határán

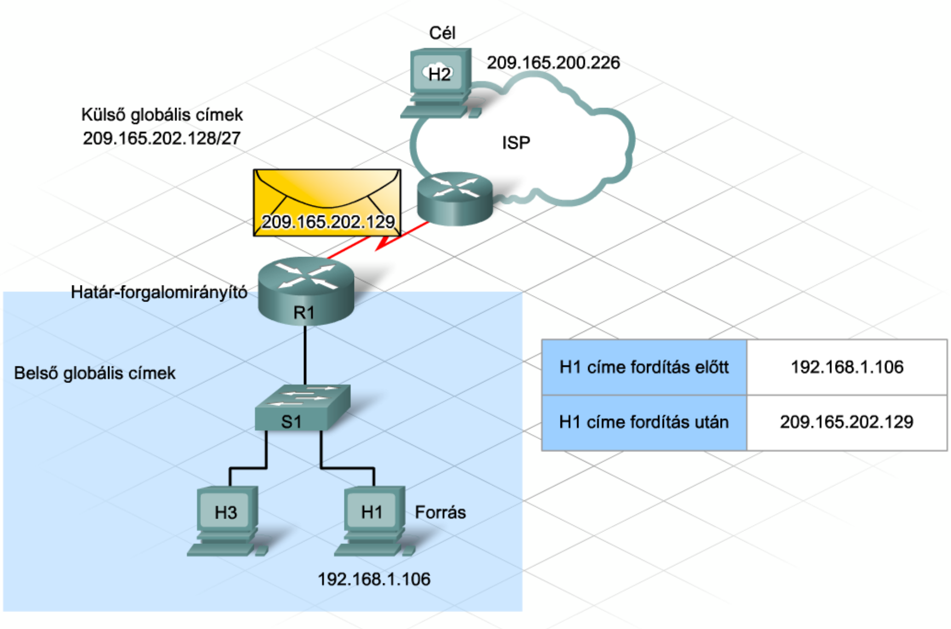
Sok szervezet az internetkapcsolat biztosításához kihasználja a privát címzés előnyeit. Számos LAN-t és WAN-t alakítanak ki privát címzéssel, és az internethez való csatlakozáshoz hálózati címfordítást (NAT) használnak.

A NAT az interneten való forgalomirányításhoz a belső privát címeket fordítja egy vagy több nyilvános címre. A NAT minden belső csomag privát forrás IP-címét az internet felé továbbítás előtt nyilvánosan bejegyzett IP-címre cseréli.

A kis és közepes méretű szervezetek saját internetszolgáltatójukhoz egyetlen kapcsolaton, a NAT-tal konfigurált helyi határ-forgalomirányítón keresztül csatlakoznak. Nagyobb szervezetek több ISP

kapcsolattal is rendelkezhetnek, ilyenkor a címfordítást az egyes kapcsolatok határ-forgalomirányítói végzik.

A határ-forgalomirányítókon alkalmazott címfordítás növeli a biztonságot. A belső privát címeket minden alkalommal egy nyilvános címre fordítják, amely elrejti a vállalat állomásainak és kiszolgálóinak az aktuális címét. A legtöbb címfordítást végző forgalomirányító blokkolja azokat a privát hálózaton kívülről érkező csomagokat, amelyek nem egy belső állomás kérésére érkező válaszok.



4.4.3 Statikus és dinamikus NAT

A NAT konfigurálható statikusan és dinamikusan is.

A statikus NAT egyetlen belső helyi címhez rendel egyetlen globális vagy nyilvános címet. Ez az összerendelés teszi lehetővé, hogy egy adott belső helyi címhez mindig ugyanaz a nyilvános cím tartozzon, és így a külső eszközök mindig elérjenek egy belső eszközt. Ilyen, a külvilágszámára is elérhető eszközök például a web- és ftp kiszolgálók.

A dinamikus NAT az internet egy nyilvános címkészletét rendeli a belső helyi címekhez. Mindig a nyilvános címkészlet első felhasználható IP-címe lesz hozzárendelve a külvilággal kommunikálni kívánó belső állomáshoz. Az állomás ezt a globális címet a kapcsolat ideje alatt használja, majd annak befejezésekor visszakerül a más állomások számára felhasználható címek közé.

Két belső állomás kapcsolatához használt cím a belső helyi cím. A vállalat nyilvános címét belső globális címnek nevezzük, amely gyakran a határ-forgalomirányító külső interfészének címe.

A NAT forgalomirányító címpárokat tartalmazó tábla segítségével kezeli a belső helyi címek és a belső globális címek közötti megfeleltetéseket.

Statikus vagy dinamikus NAT konfigurálása során:

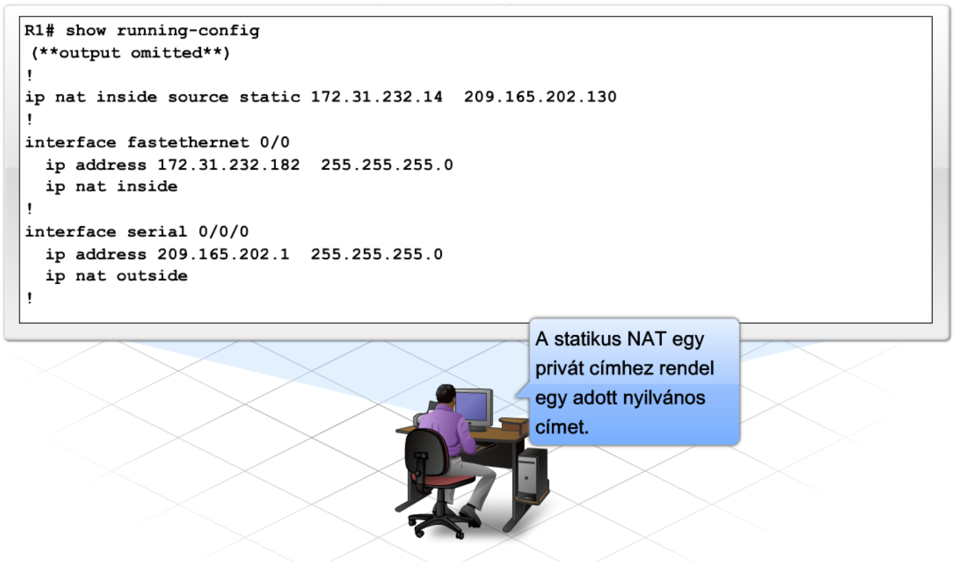
- Vegyük számba azokat a kiszolgálókat, amelyek állandó külső címet igényelnek!

- Határozzuk meg mely belső állomások igényelnek címfordítást!
- Határozzuk meg, mely interfészekre érkezik a külvilág felé irányuló belső forgalom! Ezek lesznek a belső interfészek.
- Határozzuk meg, melyik interfész továbbítja a forgalmat az internet felé! Ez lesz a külső interfész.
- Határozzuk meg a felhasználható nyilvános címtartományt!

Statikus NAT konfigurálása

1. Határozzuk meg azt a nyilvános IP-címet, amelyet a külső felhasználók használhatnak a belső eszköz vagy kiszolgáló eléréséhez! A rendszergazdák erre a célra leggyakrabban a statikus NAT címtartomány első vagy utolsó címeit használják. Végezzük el a belső vagy privát címek nyilvános címekhez rendelését!

2. Állítsuk be a belső és külső interfészeket!



Dinamikus NAT konfigurálása

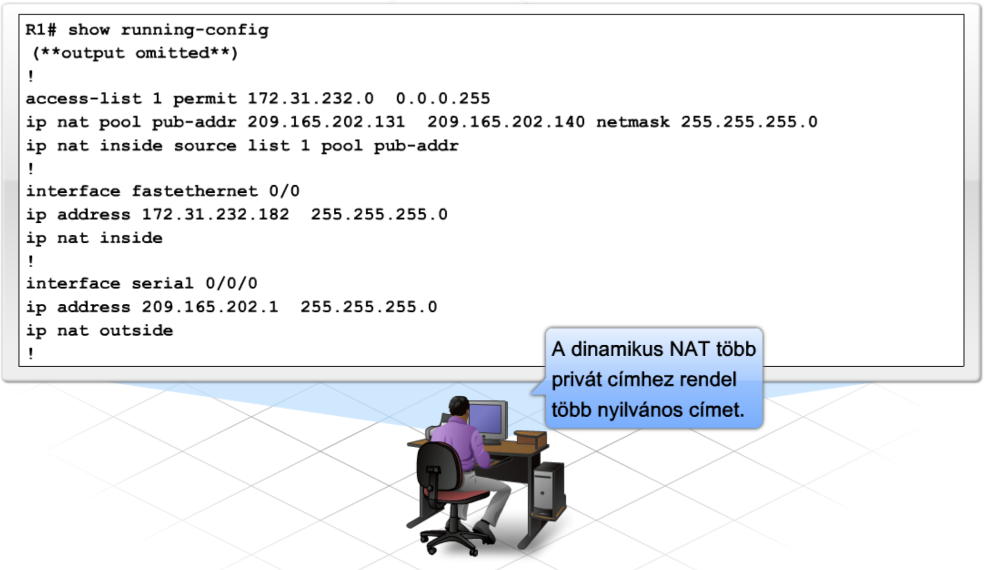
1. Határozzuk meg a felhasználható nyilvános IP-címkészletet!

2. Hozzunk létre hozzáférési-listát (ACL) a címfordítást igénylő állomások meghatározásához.

3. Állítsuk be a belső és a külső interfészeket.

4. Rendeljük hozzá a címkészlethez a hozzáférési listát!

A dinamikus NAT konfigurálásának fontos része a normál hozzáférési listák alkalmazása. A normál hozzáférési-lista engedélyező és tiltó utasításokkal határozza meg azokat az állomásokat, amelyek címfordítást igényelnek. A hozzáférési lista vonatkozhat egy egész hálózatra, egy alhálózatra vagy csak egy adott állomásra. Terjedelmét tekintve állhat egyetlen sorból vagy számos engedélyező és tiltó parancsból.



4.4.4 A PAT használata

A dinamikus NAT egyik leggyakrabban alkalmazott változata a portcímfordítás (PAT – Port Address Translation), vagy más néven túlterhelt NAT. A PAT dinamikusan egyetlen nyilvános címre fordít több belső helyi címet.

Amikor a forrásállomás üzenetet küld a célállomásnak, egy IP-címet és egy portszámot használ minden egyes párbeszéd követésére. PAT esetén a határ forgalomirányító a helyi forráscím és portszám párt fordítja le egyetlen nyilvános IP-címre és egy1024 fölötti egyedi portszámra.

A forgalomirányító egy táblában tartja nyilván a külső címre fordított belső IP-cím és portszám párokat. Bár minden állomás címét ugyanarra a globális címre fordítja, a párbeszédekhez rendelt portszámok egyediek lesznek.

Mivel több, mint 64000 port használható, így nem valószínű, hogy egy forgalomirányító kiosztható címei elfogynak.

Mind vállalati, mind otthoni hálózatok kihasználják a PAT működésének előnyeit. A PAT az integrált forgalomirányítók alapfunkciói közé tartozik, és alapértelmezetten engedélyezett.

Annak ellenére, hogy a PAT egy címtartomány helyett egyetlen címre fordít, konfigurációja ugyanazokkal az alapvető lépésekkel és parancsokkal történik, mint a NAT konfigurációja. A következő parancs a belső címeket fordítja a soros interfész IP-címére:

```
ip nat inside source list 1 interface serial 0/0/0 overload
```

A NAT és PAT működésének ellenőrzésére szolgáló parancsok:

```
show ip nat translations
```

A parancs az aktív fordításokat mutatja. A nem használt címfordítások adott idő után kiöregednek. Míg a statikus NAT-bejegyzések folyamatosan a NAT-táblában maradnak, addig a dinamikus bejegyzéshez az állomás és a külső hálózatbeli célállomás között valamilyen aktivitásra van szükség. Megfelelő beállítás mellett, egy egyszerű ping vagy trace parancs is bejegyzést eredményez a NAT-táblába.

```
show ip nat statistics
```

A parancs a fordítások statisztikáját mutatja, beleértve a használt IP-címek számát, valamint a sikeres és sikertelen fordításokat. A kimenet tartalmazza továbbá a belső címeket meghatározó hozzáférési listát, a nyilvános címkészletet és a megadott címtartományt.

4.5 A fejezet összefoglalása

- Egyetlen szórási tartomány esetén nem hierarchikus vagy egyszintű hálózatról beszélünk.
- A hierarchikus címzés a hálózatokat logikailag bontja kisebb alhálózatokra.
- A hierarchikus hálózattervezés egyszerűsíti a hálózat felügyeletét, növeli skálázhatóságát és teljesítményét.
- Alapszintű vagy szabványos alhálózatokra bontás esetén minden alhálózat ugyanakkora méretű és ugyanannyi állomás címzésére alkalmas.
- Változó hosszúságú alhálózati maszk (Variable Length Subnet Masking - VLSM) esetén az útvonalak összevonásával csökkenthető az irányítótáblák mérete.
- A VLSM lehetővé teszi minden alhálózatban különböző maszk használatát.
- Az alhálózatok tovább bonthatók al-alhálózatokra.
- A VLSM osztály nélküli irányító protokoll használatát igényli.
- VLSM megvalósításakor figyelembe kell venni az alhálózatok és a szükséges állomások számának várható növekedését.
  - Osztály alapú IP-címzés egy hálózati cím alhálózati maszkját az első oktett értéke alapján határozza meg.
  - CIDR esetén a hálózati címet nem a cím osztálya határozza meg, hanem a prefix hossz.
  - Az útvonal-összevonás a folytonos alhálózatokat egyetlen cím és egy rövidebb maszk segítségével csoportosítja, ezzel csökkentve a hirdetett útvonalakat.
  - Az útvonal-összevonás, útvonal összegzés vagy szuperhálózat készítés a hálózat határán a határ-forgalomirányítón történik.
  - Osztály alapú irányító protokollok használata nem folytonos hálózatok kialakulásához vezethet.
- A privát címek belső hálózaton használhatók és irányíthatók, de nem irányíthatók az interneten.
- A NAT a privát címeket fordítja az internet felé vezető nyilvános címekre.
- A statikus NAT egyetlen belső helyi címhez rendel egy belső globális (nyilvános) címet.
- A dinamikus NAT egy nyilvános címkészletből rendel címeket a belső helyi címekhez.
- A PAT több helyi címet fordít át egyetlen globális IP-címre.

5. Forgalomirányítás távolságalapú irányító protokollal

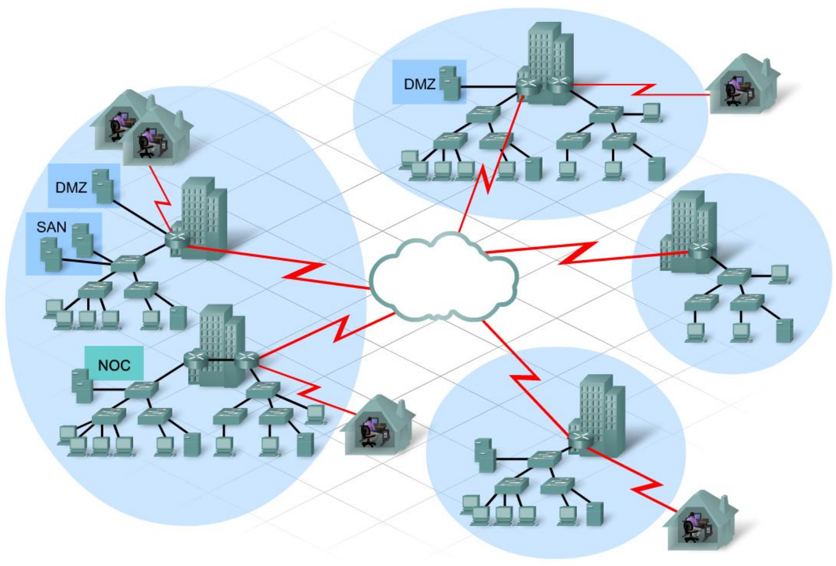
5.1 Nagyvállalati hálózatok karbantartása

5.1.1 Nagyvállalati hálózatok

A nagyvállalati hálózatok hierarchikus felépítése megkönnyíti a vállalaton belüli információáramlást. Az információ a fiókirodák és a távoli (mobil) alkalmazottak között áramlik. Ezek a fiókirodák a központi irodákhoz kapcsolódnak szerte a világban. A vállalat egyes részeinek eltérő hálózati igényeit a szervezet hierarchia kiépítésével próbálja meg biztosítani.

A kritikus szolgáltatások és információk a hierarchia csúcsához tartozó biztonságos kiszolgálófarmokon és tárolóhálózatokon találhatók. Ez a struktúra a hierarchia alsóbb szintjein található részlegekre is kiterjedhet.

A hierarchia különböző szintjei közötti kommunikációhoz a LAN és WAN technológiák egyaránt szükségesek. A vállalat növekedésével vagy az elektronikus kereskedelmi szolgáltatások bővülésével szükség lehet a különböző funkciójú kiszolgálóknak helyet biztosító demilitarizált zóna (DMZ) létrehozására.

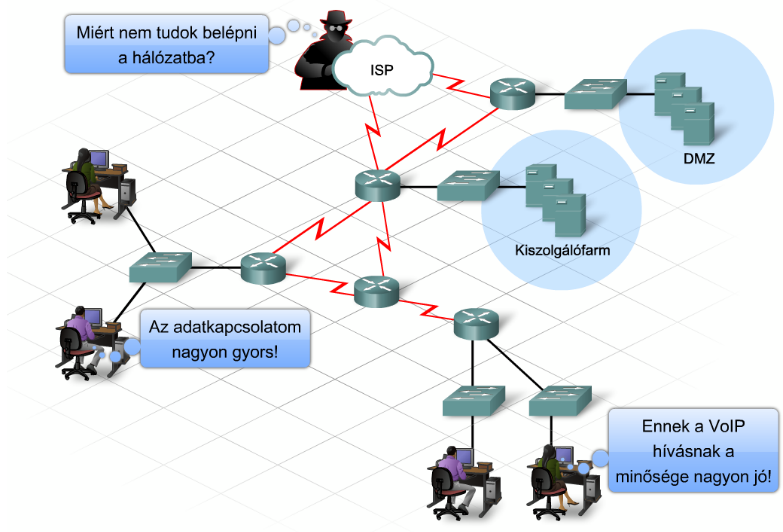


A forgalomszabályozás elengedhetetlen a nagyvállalati hálózatokban. Enélkül ezek a hálózatok nem tudnak működni.

A forgalomirányítók továbbítják az adatokat és megakadályozzák, hogy a szórásos üzenetek túlterheljék a kritikus szolgáltatások felé vezető adatvonalakat. A helyi hálózatok között úgy szabályozzák a forgalmat, hogy csak a kívánt forgalom haladhasson át a hálózaton.

A nagyvállalati hálózatok nagy megbízhatóságot és magas színvonalú szolgáltatásokat nyújtanak. Ennek biztosítására a hálózati szakemberek:

- Tartalék útvonalakat terveznek a hálózathoz, arra az esetre, ha az adatok elsődleges útvonala meghibásodna.
- Szolgáltatásminőségi eljárások bevezetésével biztosítják a kritikus adatok elsőbbségét.
- Csomagszűrést használnak bizonyos típusú csomagok letiltására, az elérhető sávszélesség maximalizálására és a hálózati támadások megelőzésére.



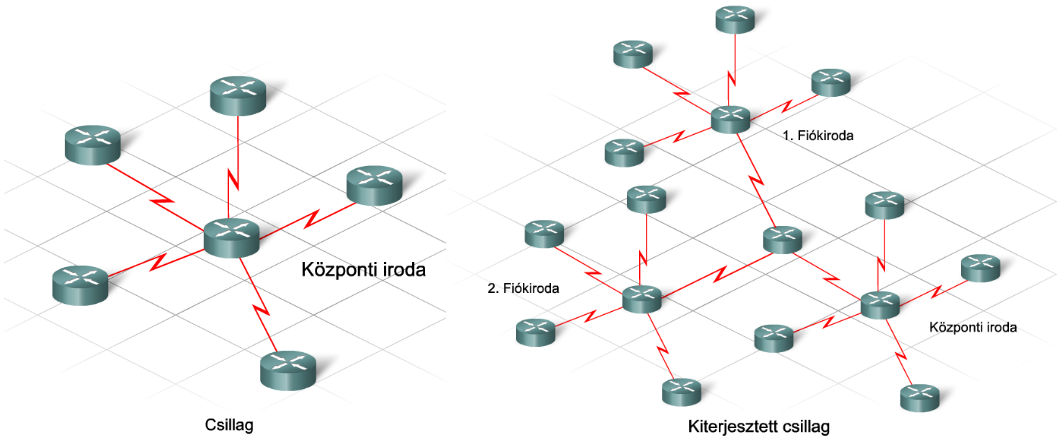
5.1.2 Nagyvállalati hálózati topológiák

A megfelelő fizikai topológia kiválasztása lehetővé teszi a vállalati hálózat szolgáltatásainak bővítését a megbízhatóság és a hatékonyság romlása nélkül. A hálózattervezők a topológia kiválasztását a vállalat megbízhatósági és hatékonysági követelményeihez igazítják. Nagyvállalati környezetben leginkább a csillag és háló topológiákat alkalmazzák.

Csillag topológia

Az egyik legnépszerűbb topológia a csillag topológia. A csillag közepe megfelel a hierarchia csúcsának, mely általában a szervezet központi irodája. A fiókirodák több helyszínről csatlakoznak a csillag központjához (hub-jához).

A csillag topológia a hálózat központosított irányítását teszi lehetővé. Így minden kritikus szolgáltatás és a technikai szakemberekből álló csapat is egy helyszínen lehet. A csillag topológiájú hálózatok egyszerűen bővíthetők. Egy új fiókiroda hozzáadása mindössze a csillag központjához történő egyetlen, új csatlakozást igényel. Ha egy iroda több új ágazatot tervez hozzáadni, akkor elég, ha minden fiókiroda a területén megtalálható központi hub-hoz csatlakozik, amely elvezet a központi iroda egyik főcsatlakozási pontjához. Így egy egyszerű csillag egy kiterjesztett csillag topológiává válik, melyben a kisebb csillagok a főirodából sugárirányokban érhetők el.



A csillag és a kiterjesztett csillag topológiában egyetlen pont (a középpont) meghibásodása a hálózat teljes működésképtelenségét okozhatja. A háló topológiájú hálózatok ezt a problémát hivatottak kiküszöbölni.

Háló Topológia

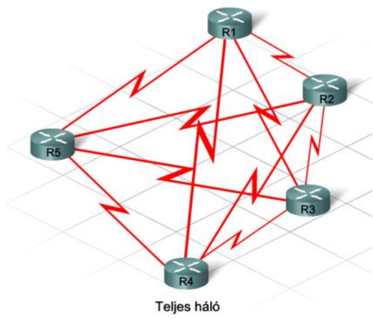
Minden újabb kapcsolat egy-egy újabb alternatív útvonalat szolgáltat az adatforgalom számára, és ezzel egyre nagyobb megbízhatóságot nyújt a hálózatnak. Újabb linkek hozzáadásával a topológia egyre inkább összekapcsolt csomópontok hálójává alakul. Ugyanakkor minden egyes újabb kapcsolat többletköltséget és többletterhelést is jelent, valamint a hálózat karbantartásának bonyolultságát is növeli.

Részleges (részben összekapcsolt) háló

A vállalati hálózat egy meghatározott részéhez adott redundáns kapcsolatokkal részleges háló topológia jön létre. Ez a topológia a hálózat olyan kritikus részeinek, mint a kiszolgálófarmok és a tárolóhálózatok, rendelkezésre állását, megbízhatóságát a többletköltségek minimalizálása mellett javítja. A hálózat többi része ugyanakkor továbbra is sérülékeny marad. Ezért nagyon fontos, hogy a redundáns vonalakat oda helyezzük, ahol azok a legtöbb előnyt nyújtják.

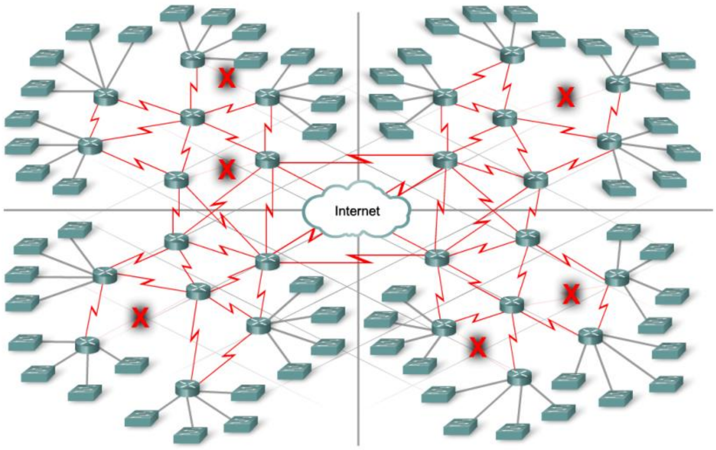
Teljes (teljesen összekapcsolt) háló

Amennyiben egy hálózatban egyáltalán nem megengedett az üzemkimaradás, akkor teljes háló topológiára van szükség. Egy teljes háló topológiában minden egyes csomópont az összes többi csomóponttal összeköttetésben van. Ez a leginkább hibaellenálló topológia, de egyben ez a legköltségesebb is



Az internet kitűnő példája a háló topológiájú hálózatoknak. Az internet eszközei nem tartoznak sem egyének, sem szervezetek hatásköre alá. A fentiek miatt az internet topológiája állandóan változik, egyes csatlakozások eltűnnek, mindeközben újabbak válnak elérhetővé. Tartalék kapcsolatok segítik a forgalomirányitást, és biztosítják a megbízható útvonalat a célállomás felé.

A nagyvállalati hálózatok hasonló problémákkal küzdenek, mint az internet. Emiatt az eszközök különböző eljárásokat használnak a folyamatosan változó körülményekhez történő alkalmazkodáshoz és a forgalom szükség szerinti átirányításához.



Folyamatosan változó hálózati környezet

5.1.3 Statikus és dinamikus forgalomirányítás

A nagyvállalati hálózatok fizikai topológiája megadja az adattovábbítás struktúráját is. A forgalomirányítás biztosítja a működéshez szükséges mechanizmust. A célhálózathoz vezető legjobb útvonal megtalálása igen bonyolult lehet egy nagyvállalati környezetben, mivel egy forgalomirányító nagyon sok forrásból építheti fel az irányítótábláját.

Az irányítótábla a RAM-ban található adatszerkezet, amely a közvetlenül kapcsolódó és a távoli hálózatokról tartalmaz információt. Az irányítótábla minden hálózatot egy kimenő interfésszel vagy egy következő ugrással azonosít.

A kimenő interfész azt a fizikai útvonalat adja meg, melyet a forgalomirányító ténylegesen az adatok célállomásra történő továbbításához használ. A következő ugrás egy közvetlenül kapcsolódó másik forgalomirányító olyan interfésze, amely a végső cél felé vezető úton található.

A tábla minden egyes útvonalhoz egy számértéket is rendel, amely az út megbízhatóságát, pontosságát jelzi. Ez az érték az adminisztratív távolság. A forgalomirányítók közvetlenül kapcsolódó, statikus és dinamikus útvonalakról tárolnak bejegyzéseket.

Közvetlenül kapcsolódó útvonalak

Egy közvetlenül kapcsolódó hálózat a forgalomirányító interfészéhez csatlakozik. Az interfészen beállított IP-cím és alhálózati maszk lehetővé teszi, hogy az interfész a csatlakozó hálózat egy állomása legyen. Az interfész hálózati címe, az alhálózati maszkja, valamint az interfész típusa és a száma az irányítótáblában, mint közvetlenül kapcsolódó hálózat jelenik meg. Az ilyen hálózatokat az irányítótáblában a „C” betű jelöli.

Statikus útvonalak

Statikus útvonalak a hálózati rendszergazda által manuálisan konfigurált útvonalak. Egy statikus útvonal tartalmazza a célhálózat hálózatcímét és hálózati maszkját, valamint a célhálózathoz vezető kimenő interfészt vagy a következő ugrás IP-címét. Az irányítótábla a statikus útvonalakat „S”-sel jelöli. A statikus útvonalak sokkal tartósabbak és megbízhatóbbak, mint a dinamikusan tanult útvonalak, így adminisztratív távolságuk is kisebb.

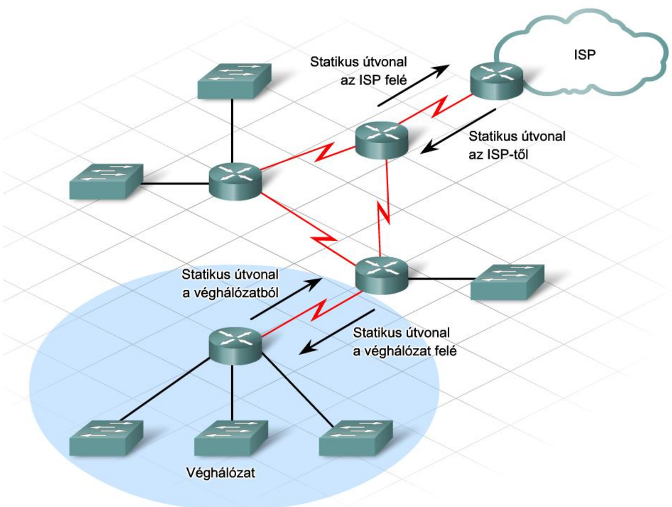
Dinamikus útvonalak

Dinamikus irányító protokollok szintén bejegyzéseket adnak hozzá az irányítótáblához a távoli hálózatokról és lehetővé teszik, hogy a forgalomirányítók a hálózat felderítése során távoli hálózatok elérhetőségéről és állapotáról osszanak meg információt. Minden irányító protokoll adatokat küld és kap más forgalomirányítókon tárolt információról, valamint frissíti és karbantartja az irányítótábláját. Minden dinamikus irányító protokoll által megtanult útvonalat a protokoll azonosít. Így például R betű azonosítja a RIP és D betű az EIGRP irányító protokollt. Az adminisztratív távolságot is ennek alapján kapja az útvonal.

Nagyvállalati hálózatokban statikus és dinamikus útvonalakat egyaránt használnak. A statikus forgalomirányítás a speciális hálózati igények miatt szükséges, valamint a fizikai topológiától függően a forgalom szabályozására is használható.

A hálózat ki- és bemenő forgalmának egyetlen pontra való korlátozása egy véghálózat, más néven zsákhálózat (stub network) létrejöttét eredményezi. Bizonyos nagyvállalati hálózatokban a kisebb fiókirodák mindössze egyetlen útvonalon képesek elérni a hálózat többi részét. Ilyen esetben nem fontos a véghálózat forgalomirányítóját irányítási frissítésekkel és a dinamikus irányító protokollokkal járó megnövekedett forgalommal terhelni. A statikus forgalomirányítás ilyenkor előnyösebb.

Elhelyezkedésüktől és feladatuktól függően bizonyos nagyvállalati forgalomirányítók szintén használhatnak statikus útvonalakat. A határátjárók általában statikus útvonalakat használnak az internetszolgáltató biztonságos és stabil elérésére, míg a nagyvállalaton belüli többi forgalomirányító az igényeknek megfelelően statikus és dinamikus forgalomirányítást egyaránt alkalmazhat.



A nagyvállalati hálózatban használt forgalomirányítóknak sávszélességre, operatív memóriára és feldolgozó erőforrásra egyaránt szükségük van a NAT/PAT-, a csomagszűrési- és az egyéb szolgáltatásaik biztosításához. Ezzel szemben a statikus forgalomirányítás a legtöbb dinamikus irányító protokollnál fellépő többletterhelés nélkül nyújt továbbítási funkciót.

Ezen felül a statikus forgalomirányítás a dinamikusnál nagyobb adatbiztonságot nyújt, mivel nincs szüksége irányítási frissítésekre. Egy hekker bármikor elfoghat egy dinamikus irányítási frissítést, és így információt szerezhet a hálózatról.

A fentiek ellenére a statikus forgalomirányítás is együtt járhat bizonyos problémákkal. A hálózati rendszergazdától időt és odafigyelést igényel, mivel a forgalomirányítási információt manuálisan kell begépelnie. Egy statikus útvonal egyszerű elgépelési hibája csomagvesztést és a hálózat működésképtelenségét okozhatja. Amikor egy statikus útvonal megváltozik, a manuális konfigurációfrissítés ideje alatt a hálózatban irányítási hibák jelentkezhetnek. Statikus útvonalak nagyvállalati hálózatban történő általános alkalmazása a fentiek miatt nem praktikus.

	Statikus forgalomirányítás	Dinamikus forgalomirányítás
Konfigurálás bonyolultsága	A hálózat méretével növekszik	Általában független a hálózat méretétől
Topológia változások	Rendszergazda beavatkozása szükséges	Automatikusan alkalmazkodik a topológia változásokhoz
Skálázhatóság	Egyszerűbb topológia esetén alkalmas	Egyszerű és bonyolult topológiák esetén is alkalmas
Biztonság	Biztonságosabb	Kevésbé biztonságos
Erőforrás használat	Semmilyen extra erőforrásra nincs szükség	CPU-t, memóriát és sávszélességet használ
Kiszámíthatóság	A célállomáshoz vezető útvonal mindig ugyanaz	Az útvonal az aktuális topológiától függ

5.1.4 Statikus útvonalak konfigurálása

Statikus útvonalak konfigurálására használt globális parancs az `ip route` kulcsszavakkal kezdődik, melyet a célhálózat címe, az alhálózati maszkja és az eléréséhez használt útvonal követ. A teljes parancs:

```
Router(config)#ip    route    [hálózati-cím]    [[alhálózati_maszk]
[[következő_ugrás_címe VAGY kimenő_interfész]
```

A forgalomirányítók a következő ugrás IP-címét vagy a kimenő interfészt használva továbbítják a csomagokat a megfelelő célállomásnak. A két paraméter mégis különbözőképpen viselkedik.

Mielőtt egy forgalomirányító továbbítja a csomagot, meg kell határozni a kimenő interfészt. Kimenő interfésszel konfigurált statikus útvonalak csak egyszeri keresést igényelnek az irányítótáblában, míg a következő ugrással megadott útvonalak esetén kétszer is szükség van az irányítótábla átvizsgálására.

Nagyvállalati hálózatokban a pont-pont összeköttetésekhez (például egy határátjáró és a szolgáltató (ISP) közötti kapcsolathoz) a statikus útvonalaknak kimenő interfésszel történő megadása a legjobb választás.

Következő ugrással megadott statikus útvonalak esetén két lépés szükséges a kimenő interfész meghatározásához. Ezt hívjuk rekurzív keresésnek. Rekurzív keresés esetén:

- A forgalomirányító először kiválasztja a csomag célcíméhez illeszkedő statikus útvonalat.
- Ezután a kimenő interfészt határozza meg oly módon, hogy az irányítótáblájában megkeresi a statikus útvonalban megadott következő ugrás címéhez tartozó bejegyzést.

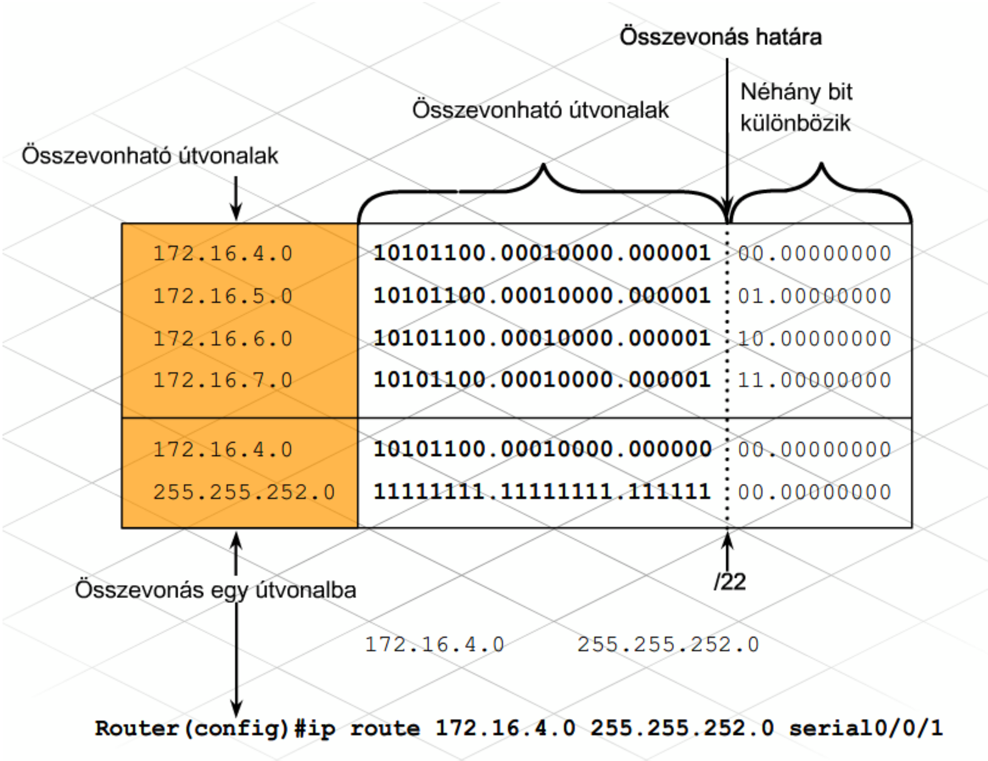
Ha egy kimenő interfész elérhetetlenné válik, akkor az érintett statikus útvonal eltűnik az irányítótáblából, majd az interfész helyreállása után újra bekerül oda.

Több statikus útvonal egyetlen bejegyzéssé egyesítése csökkenti az irányítótábla méretét és hatékonyabbá teszi a keresési folyamatot. Ezt a folyamatot útvonal összevonásnak (útvonal összegzésnek) nevezzük.

Egy statikus útvonal több statikus útvonalat egyesít, ha:

- A célhálózatokat egy hálózati cím fogja össze.
- Mindegyik statikus útvonal ugyanazt a kimenő interfészt vagy következő ugrás IP-címét használja.

Útvonalösszegzés nélkül, az irányítótáblák az internet gerinchálózatának forgalomirányítóiban kezelhetetlenek lennének. A nagyvállalati hálózatokban is hasonló probléma jelentkezhet. Az összevont statikus útvonalak alkalmazása elengedhetetlen ahhoz, hogy nagy hálózatokban az irányítótáblák mérete kezelhető méretű maradjon.



A vállalati hálózatokban használt WAN-szolgáltatások kialakításától függően a statikus útvonalak tartalék útvonalként is funkcionálhatnak, ha az elsődleges WAN kapcsolat kiesik. Az ún. lebegő statikus útvonalak (floating static route) biztosítják ezt a tartalék útvonal szolgáltatást.

Alapértelmezett beállításnál egy statikus útvonalnak kisebb az adminisztratív távolsága, mint egy dinamikusan tanult útvonalnak. A lebegő statikus útvonalnak az adminisztratív távolsága nagyobb, mint a dinamikus irányító protokoll által tanult útvonalénak, így nem kerül be az irányítótáblába, csak a dinamikusan tanult útvonal kiesése esetén.

A lebegő statikus útvonal létrehozásához az ip route parancs végére adjunk meg egy adminisztratív távolság értéket:

```
Router(config)#ip route 192.168.4.0 255.255.255.0 192.168.9.1 200
```

A megadott adminisztratív távolságnak nagyobbnak kell lennie, mint a dinamikus irányító protokoll által tanult útvonalénak. A forgalomirányító mindaddig az elsődleges útvonalat fogja használni, ameddig az aktív. Ha az elsődleges útvonal valamilyen oknál fogva kiesik, akkor az irányítótáblába bekerül a lebegő statikus útvonal.

5.1.5 Alapértelmezett útvonalak

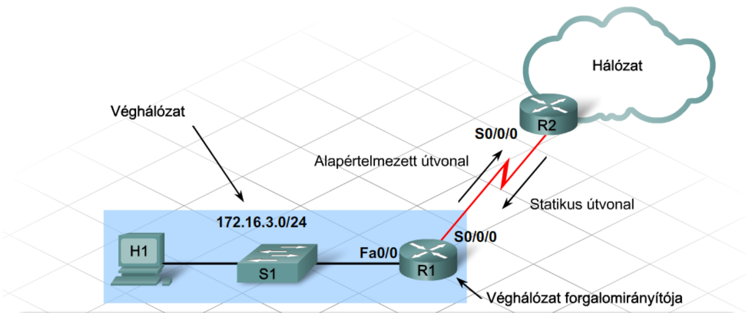
Az irányítótáblák nem tudnak minden egyes internet címhez bejegyzést eltárolni. Minél nagyobb az irányítótábla mérete, annál több RAM–ot és feldolgozási időt igényel. Az alapértelmezett útvonal a statikus útvonal egy olyan különleges típusa, ami egy átjárót határoz meg arra az esetre, ha az irányítótábla nem tartalmaz bejegyzést a célhálózathoz. Általában az alapértelmezett útvonalak az ISP felé vezető út legközelebbi forgalomirányítójára mutatnak. Bonyolult nagyvállalatok esetén az alapértelmezett útvonalak az internetes forgalmat kifelé irányítják a hálózatból.

Az alapértelmezett útvonalak létrehozására szolgáló parancs hasonlít a hagyományos vagy lebegő statikus útvonalakéhoz, azzal a különbséggel, hogy ebben az esetben a hálózati cím és az hálózati maszk értéke egyaránt 0.0.0.0 („négy 0-s” útvonal). A parancs vagy a következő ugrás IP-címét vagy a kimenő interfészt használja paraméterként.

A nullák jelzik a forgalomirányító számára, hogy nincs szükség a bitek egyezésére az útvonal használatához. Mindaddig, amíg jobb egyezés nem létezik a forgalomirányító az alapértelmezett statikus útvonalat fogja használni.

A határátjárón létrehozott alapértelmezett útvonal a forgalmat az ISP felé továbbítja. Ez az útvonal azonosítja a nagyvállalaton belüli utolsó megállót, az olyan csomagok végső átjáróját (Gateway of Last Resort), amelyek célcíme egyetlen irányítótábla bejegyzéssel sem egyezik. Ez az információ minden forgalomirányító irányítótáblájában megjelenik.

Ha a vállalat dinamikus forgalomirányító protokollt használ, akkor a határátjárók az alapértelmezett útvonalat az irányítási frissítések részeként is elküldhetik a többi forgalomirányítónak.




```
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
R1(config)#end

R1#show ip route
(**output omitted**)

        Gateway of last resort is 0.0.0.0 to network 0.0.0.0

        172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S       0.0.0.0/0 is directly connected, Serial0/0/0
```

5.2 RIP protokollal történő forgalomirányítás

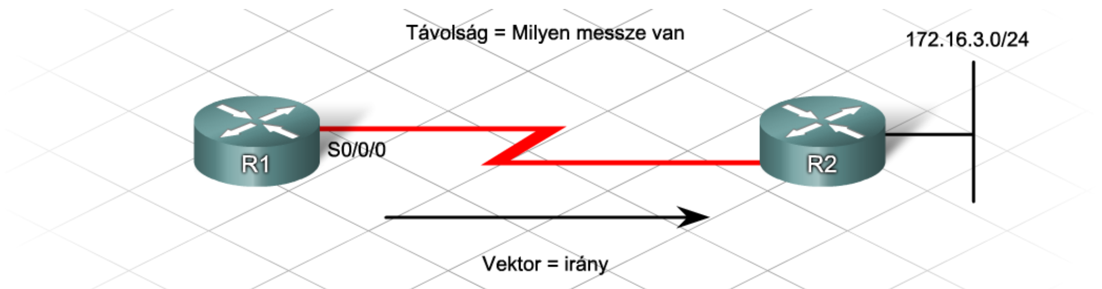
5.2.1 Távolságvektor alapú forgalomirányító protokollok

A dinamikus irányító protokollok két fő kategóriába sorolhatók: Távolságvektor alapú – és kapcsolatállapot alapú protokollok.

Távolságvektor alapú irányító protokollt futtató forgalomirányítók a hálózati információt a közvetlenül kapcsolódó szomszédjaikkal osztják meg. A szomszédos forgalomirányítók továbbítják az információt az ő szomszédjaiknak, mindaddig, míg a vállalat minden forgalomirányítójához el nem jut az információ.

Egy távolságvektor alapú irányító protokollt futtató forgalomirányító nem ismeri a célállomásig terjedő teljes útvonalat, csak a távoli hálózat távolságát és irányát, azaz vektorát. Az összes információja a közvetlenül kapcsolódó szomszédjaitól származik.

A többi irányító protokollhoz hasonlóan a távolságvektor alapú irányító protokollok is egy mértéket (mérőszámot) használnak a legjobb útvonal meghatározására. A távolságvektor alapú irányító protokollok a legjobb útvonalat a forgalomirányító és a célhálózat közötti távolság alapján számolják. A leggyakrabban használt mérték az ugrásszám, mely a forgalomirányító és a célállomás közötti forgalomirányítók száma.



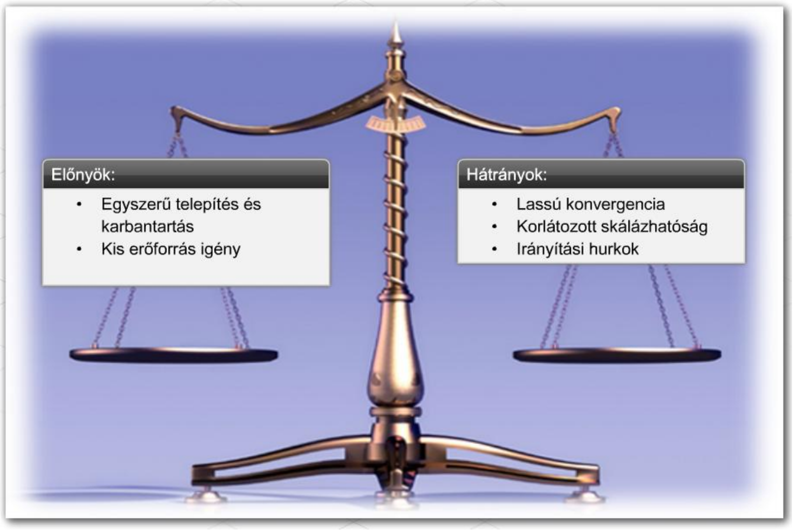
Az R1 forgalomirányító felől nézve a 172.16.3.0/24 hálózat egy ugrás távolságra van. Az S0/0/0 interfészen keresztül az R2 forgalomirányító felé érhető el.

A távolságvektor alapú irányító protokollok általában kevesebb és egyszerűbb konfigurálást és karbantartást igényelnek, mint a kapcsolatállapot alapúak. Régebbi verziójú, kevésbé erőteljes forgalomirányítón is képesek futni és kevesebb memóriát és feldolgozási teljesítményt igényelnek.

Távolságvektor alapú protokollt futtató forgalomirányítók rendszeres időközönként a teljes irányítótáblájukat elküldik a szomszédos forgalomirányítóknak szórásos vagy csoportos küldés segítségével. Ha egy forgalomirányító több útvonalat is ismer egy célhálózathoz, akkor a legkisebb mértékű utat hirdeti.

Az irányítási információk nagy hálózatokban történő ilyen jellegű továbbítása lassú. Bármelyik pillanatban létezhetnek olyan forgalomirányítók, melyek nem rendelkeznek a legfrissebb információval a hálózatról. Ez a protokollok skálázhatóságát korlátozza és olyan problémák, mint az irányítási hurkok kialakulását is okozhatja.

A RIP irányító protokoll 1. és 2. verziója igazi távolságvektor alapú protokoll, míg az EIGRP lényegében egy távolságvektor alapú protokoll továbbfejlesztett lehetőségekkel. A RIPng-t, a RIP legújabb változatát kifejezetten az IPv6 támogatására fejlesztették ki.



5.2.2 Forgalomirányítási információs protokoll (Routing Information Protocol, RIP)

A forgalomirányítási információs protokoll (RIP) volt az első RFC-ben (az 1988-ban kiadott RFC 1058-ban) szabványosított távolságvektor alapú IP irányító protokoll. Az első verziót gyakran RIPv1-nek hívják, megkülönböztetésül a későbbi javított verziótól, a RIPv2-től és az IPv6-ot támogató RIPng-től.

Alapértelmezett beállításoknál a RIPv1 30 másodpercenként küld irányítási frissítéseket minden aktív interfészen szórással.

A RIPv1 osztály alapú irányító protokoll. Automatikusan összegzi az alhálózatokat az osztály határokon és a frissítésekben nem küld alhálózati maszkot. A fentiek miatt nem támogatja a változó hosszúságú alhálózati maszkok használatát (VLSM) és az osztályok nélküli, körzetek közötti forgalomirányítást (CIDR). Egy RIPv1-gyel konfigurált forgalomirányító vagy a helyi interfészén beállított alhálózati maszkot, vagy az alapértelmezett osztály alapú maszkot használja. A RIPv1-el hirdetett alhálózatoknak a megfelelő forgalomirányítás érdekében folytonosaknak kell lenniük.

Például egy forgalomirányító, melynek két interfésze a 172.16.1.0/24 és a 172.16.4.0/24 hálózatok átjárójaként működik, RIPv1-el csak a 172.16.0.0 B osztályú hálózatot fogja hirdetni. Egy másik forgalomirányító, mely megkapja ezt a frissítést csak a 172.16.0.0 B osztályú hálózatot fogja az irányító táblájában megjeleníteni. Így egy 172.16.3.0–ás célhálózatú csomag tévesen a 172.16.0.0 B osztályú hálózatot hirdető forgalomirányítóhoz kerülhet, melynek eredményképpen a megfelelő célcímre nem érkezik meg.

A RIPv2 sok tulajdonságában hasonlít a RIPv1-hez, de fontos újításokat is tartalmaz. A RIPv2 egy osztály nélküli irányító protokoll, mely támogatja a változó hosszúságú alhálózati maszkok használatát (VLSM) és az osztályok nélküli, körzetek közötti forgalomirányítást (CIDR). A 2. verziójú frissítések tartalmazzák az alhálózati maszkot, így nem folytonos hálózatok használata is megengedett RIPv2-t használó hálózatokban. Ezen felül a RIPv2 esetén kikapcsolható az automatikus hálózat összegzési funkció.

A RIP mindkét verziója minden konfigurált interfészén kiküldi a teljes irányítótáblát. Alapbeállitásban a RIPv1 a 255.255.255.255 címet használó szórásos küldés (broadcast) segítségével küldi a frissítéseket. Ez az olyan szórásos hálózatok esetén, mint az Ethernet, a hálózat összes állomása számára az adatok feldolgozását igényli. A RIPv2 csoportos küldés (többes küldés, multicast) segítségével hirdeti frissítéseit a 224.0.0.9-es címen. A csoportos küldés kevesebb sávszélességet foglal le, mint a szórás. Azok az eszközök, melyeken nincs RIPv2 konfigurálva az adatkapcsolati rétegben, eldobják a csoportos küldéses csomagokat.

A támadók gyakran helytelen frissítések küldésével érik el, hogy a forgalomirányítók az adatokat rossz címre küldjék, illetve hogy a hálózat teljesítőképessége komoly mértékben csökkenjen. Helytelen információ hibás konfiguráció vagy működési zavar miatt is bekerülhet az irányítótáblába. Az irányítási információk titkosítása az irányítótáblák tartalmát elrejti a jelszóval vagy a hitelesítő információval nem rendelkező forgalomirányítók elől. A RIPv2 a RIPv1-el ellentétben rendelkezik hitelesítő eljárással.

Bár a RIPv2 számos továbbfejlesztést tartalmaz, mégsem tekinthető teljesen különböző protokollnak. A két verziónak több, a következőkben felsorolt közös tulajdonsága létezik:

- Az ugrásszám a mérték
- 15 ugrás a maximum
- A TTL értéke 16 ugrás
- Alapértelmezetten 30 másodpercesek a frissítési intervallumok
- Útvonalmérgezést, visszirányú mérgezést, láthatármegosztást és visszatartó számlálókat használnak az irányítási hurkok kiküszöbölésére
- Frissítésekhez az UDP 520-as portját használják
- Az adminisztratív távolság értéke 120
- Az üzenet fejrésze maximum 25 hitelesítés nélküli útvonalat tartalmaz

Egy forgalomirányító a bekapcsolása után minden RIP protokollal konfigurált interfészén egy kérést küld a protokollban résztvevő szomszédoknak, hogy küldjék el a teljes irányítótábla tartalmát. A RIP protokollal konfigurált szomszédok az általuk ismert hálózatok bejegyzéseinek elküldésével válaszolnak. A fogadó forgalomirányító minden egyes útvonalat a következő kritériumok alapján értékel:

- Ha a kapott útvonal ismeretlen, akkor a forgalomirányító beírja az irányítótáblájába.
- Ha az útvonalra már található bejegyzés az irányítótáblában egy másik forrástól, akkor az újat csak akkor írja be, ha az jobb ugrásszámmal rendelkezik a réginél.
- Ha az útvonal már a táblában van és ugyanattól a forrástól származik, akkor mindenképpen kicseréli az új bejegyzésre, még akkor is, ha a mérték nem jobb.

A frissen bekapcsolt forgalomirányító ezután egy eseményvezérelt frissítést küld a RIP protokollal konfigurált interfészein a saját irányítótáblája tartalmának elküldésével, így a RIP szomszédok az összes új útvonalról értesülnek.

Ha a forgalomirányítók a megfelelő verziójú frissítéseket küldik és dolgozzák fel, akkor a RIPv1 és RIPv2 teljesen kompatibilisek egymással. Alapértelmezésben a RIPv2 csak 2. verziójú frissítéseket küld és fogad. Ha egy hálózatban mindkét verziót kell használni, akkor a hálózati rendszergazda konfigurálhatja úgy a RIPv2-t, hogy 1. és 2. verziójú frissítést egyaránt küldjön és fogadjon. A RIPv1 alapértelmezésben 1. verziójú frissítéseket küld, de mindkettőt fogadja.

Egy nagyvállalaton belül szükség lehet a RIP mindkét verziójának használatára. Például, míg a hálózat egy része áttért a 2. verzióra, addig lehet, hogy egy másik része megmaradt az eredeti verziónál. A globális RIP konfiguráció kiegészítése interfész-specifikus tulajdonságokkal lehetővé teszi a két verzió együttes használatát.

A globális konfiguráció interfészen történő testre szabásához használja a következő interfész konfigurációs parancsokat:

```
ip rip send version <1 | 2 | 1 2>
ip rip receive version <1 | 2 | 1 2>
```

5.2.3 RIP konfigurálása

A RIP konfigurálása előtt be kell állítani a forgalomirányításban résztvevő interfészek IP-címeit és maszkjait, valamint az órajelet azokon a soros összeköttetéseken ahol szükséges. Az alapszintű beállítások után kerülhet sor a RIP konfigurálására.

A RIP alapvető konfigurálása három parancsból áll:

```
Router(config)#router rip
```

- Az irányító protokoll engedélyezése

```
Router(config)#version 2
```

- A verzió megadása

```
Router(config-router)#network [hálózati cím]
```

- Az összes közvetlenül kapcsolódó, RIP hirdetésben résztvevő hálózat megadása

Az MD5 autentikáció konfigurálásához a RIPv2 protokollban résztvevő interfészeken ki kell adni az ip rip authentication mode md5 parancsot.

Ennek a parancsnak a hatására az adott interfészen kimenő összes frissítés titkosítva lesz.

A RIPv2 egy alapértelmezett útvonalat is képes elküldeni a frissítéseiben a szomszédos forgalomirányítóknak. Ehhez szükség van az alapértelmezett útvonal konfigurálására és a RIP konfiguráció redistribute static paranccsal történő kiegészítésére.

5.2.4 A RIP problémái

Számos teljesítménybeli és biztonsági probléma vetődik fel a RIP használatakor. Az első probléma az irányítótábla pontossága.

A RIP mindkét verziója automatikusan összegzi a hálózatokat az osztály határokon. Ez azt jelenti, hogy a RIP az alhálózatokat, mint egyedi A, B és C osztályú hálózatok ismeri fel. Nagyvállalati hálózatok tipikusan osztály nélküli címzést használnak, valamint alhálózatok sokaságát, melyek olykor nem összefüggő alhálózatokat alkotnak, mivel nem mindig kapcsolódnak közvetlenül egymáshoz.

A RIPv1-el ellentétben a RIPv2 esetében az automatikus összegzés kikapcsolható. Ebben az esetben a RIPv2 minden alhálózatot külön hirdet a megfelelő maszkkal együtt, így pontosabb irányítótáblát biztosít. Ehhez a RIPv2 konfiguráció no auto-summary paranccsal történő kiegészítése szükséges.

```
Router(config-router)#no auto-summary
```

Egy másik problémát okoz a RIPv1 frissítések szórásos jellege. Amint a RIP konfigurációban megadtunk legalább egy network parancsot, a RIP azonnal elkezdi küldeni a frissítéseit network parancsban megadott hálózathoz tartozó interfészein. Ezekre a frissítésekre nincs szükség a hálózat minden részén. Például ezeknek a frissítéseknek egy Ethernet LAN interfészen keresztül a hálózat összes eszközének történő kiküldése felesleges hálózati forgalmat okozhat az adott szegmensen. Ráadásul ezeket a frissítéseket bármely eszköz elfoghatja, s ez a hálózat biztonságát is csökkenti.

Az interfész konfigurációs módban kiadott passive-interface parancs a parancsban megadott interfészen letiltja az irányítási frissítések kiküldését.

```
Router(config-router)#passive-interface interfész_típus
interfész_szám
```

A több irányító protokollt is használó, bonyolult nagyvállalati hálózatokban a passive-interface paranccsal megadható mely forgalomirányítók kapják meg a RIP útvonalakat. A RIP útvonalakat hirdető interfészek számának korlátozása nagyobb mértékű biztonsághoz és forgalomszabályozáshoz vezet.

Egy RIP-et használó hálózatban időre van szükség a konvergenciához. A forgalomirányítók helytelen útvonalakat is tárolhatnak az irányítótábláikban mindaddig, amíg az összes forgalomirányító nem frissítette az irányítótábláját, és ugyanazt a képet nem látják a hálózatról.

A hibás hálózati információ az irányítási frissítések és más forgalmak végtelen hurokba kerülését okozhatja. RIP irányító protokoll esetén a „végtelent” a 16 ugrásszám jelenti.

Az irányítási hurkok rontják a hálózat teljesítményét. A RIP számos lehetőséget tartalmaz ennek a hatásnak a kiküszöbölésére, melyeket akár egyszerre is alkalmazhatnak:

- Visszirányú mérgezés
- Látóhatármegosztás

- Visszatartó időzítők
- Eseményvezérelt frissítések

A visszirányú mérgezés az útvonal mértékét 16-ra állítja, s így elérhetetlennek nyilvánítja azt. Mivel a RIP a végtelent 16-nak definiálja, ezért minden olyan hálózat mely 15 ugrásnál távolabb van elérhetetlennek minősül. Ha egy hálózat elérhetetlen, akkor a forgalomirányító megváltoztatja arra az útvonalra vonatkozó mértéket 16-ra, hogy minden más forgalomirányító is elérhetetlennek lássa. Ez a tulajdonság akadályozza meg a mérgezett útvonalakon küldött információk terjedését

A RIP hurokmentesítési megoldásai stabil működést eredményeznek, ugyanakkor a hálózat konvergencia idejét növelik.

A látóhatármegosztás megakadályozza a hurkok kialakulását. Ha több forgalomirányító is ugyanazt az útvonalat hirdeti egymásnak, akkor irányítási hurok jöhet létre. A láthatármegosztás megakadályozza, hogy egy forgalomirányító azon az interfészén hirdessen egy útvonalat, amelyiken azt megismerte.

A visszatartó számlálók stabilizálják az útvonalakat. A visszatartó időzítők ugyanis megakadályozzák egy leállt útvonalra vonatkozó frissítésnek az elfogadását, ha a frissítés a leállást követő meghatározott időintervallumon belül érkezik, és nagyobb mértéket szerepel benne a korábbi értéknél. Ha a visszatartó időzítő lejárta előtt az eredeti útvonal helyreáll, vagy a forgalomirányító olyan útvonal információt kap, mely kisebb mértékkel rendelkezik, akkor a forgalomirányító felveszi az irányítótáblájába, és azonnal használni is kezdi.

Az alapértelmezett visszatartási idő 180 másodperc, a rendszeres frissítési idő hatszorosa. Az alapértelmezett érték megváltoztatható, de a visszatartási intervallum növelése lassabb hálózati konvergenciát okoz, és negatív hatással bír a hálózati teljesítményre.

Ha egy útvonal kiesik, a RIP nem várja meg a következő frissítési időt, hanem azonnal küld egy rendkívüli frissítést, amit eseményvezérelt frissítésnek nevezünk. A kiesett útvonalat 16-os mértékkel hirdeti, igy az utat megmérgezi. Ez a frissítés visszatartási állapotban tartja az útvonalat, mindaddig amíg a RIP egy jobb mértékű alternatív útvonalat nem talál helyette.

5.2.5 RIP ellenőrzése

A RIPv2 egy egyszerűen konfigurálható protokoll. Ennek ellenére hibák és ellentmondásos állapotok mindig keletkezhetnek egy hálózaton. Számos `show` parancs segíti a rendszergazdát a RIP konfigurációjának ellenőrzésében és a működési hibák felderítésében.

Bármely irányító protokoll esetén a `show ip protocols` és a `show ip route` parancsok fontos szerepet játszanak a hibaelhárításban.

A következő parancsok kifejezetten a RIP ellenőrzését és hibaelhárítását szolgálják:

- `show ip rip database`: Minden RIP által megismert útvonalat listáz
- `debug ip rip` vagy a `debug ip rip {events}`: A RIP által küldött és fogadott irányítási frissítéseket mutatja valós időben

Ennek a debug parancsnak a kimenete megmutatja az összes frissítés forrásának az IP-címét és interfészét, valamint a protokoll verzióját és az útvonal mértékét.

Ne használja a szükségesnél többet a debug parancsokat. A debug parancs használata nagy sávszélességi és feldolgozási erőforrás-igénnyel jár, ami lassítja a hálózatot.

A `ping` paranccsal a végponttól végpontig terjedő kapcsolatok tesztelhetők. A `show running-config` parancs segítségével kényelmes ellenőrizhetjük, hogy az összes parancsot megfelelően írtuk-e be.

5.3 Forgalomirányítás az EIGRP protokollal

5.3.1 A RIP korlátai

A RIP irányító protokollt könnyű konfigurálni, működtetéséhez minimális forgalomirányító erőforrás szükséges.

A RIP által használt egyszerű ugrásszám mérték azonban bonyolult hálózatokban nem a legoptimálisabb a legjobb útvonal megtalálásához. A RIP ezen felül 15 ugrásban maximalizálja a távoli hálózatok elérhetőségét.

A RIP az irányítótáblájáról periodikus frissítéseket küld, mely sávszélességet foglal, még akkor is, ha nem történik változás a hálózatban. A forgalomirányítóknak ezeket fogadniuk kell és fel kell dolgozniuk, hogy eldönthessék, hogy az adott üzenet tartalmaz-e friss információt.

Időt vesz igénybe, hogy a forgalomirányítóról forgalomirányítóra küldött frissítések a hálózat minden részét elérjék, így elképzelhető, hogy a forgalomirányítók nem rendelkeznek pontos információval a hálózat aktuális állapotáról. A hosszú konvergencia idő következtében irányítási hurok keletkezhet, mely értékes sávszélességet foglal le.

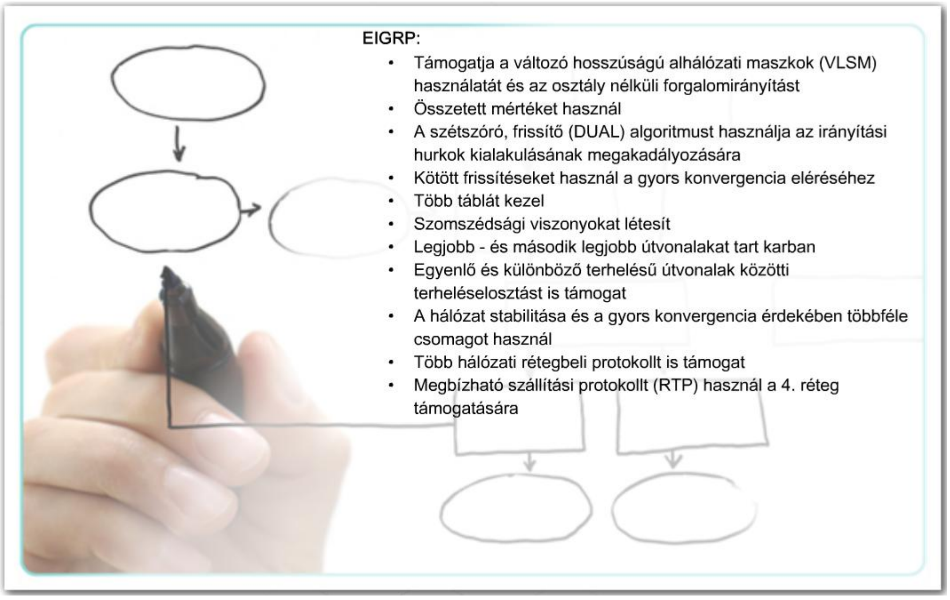
Mindezek a tulajdonságok korlátozzák a RIP irányító protokoll használhatóságát nagyvállalati környezetben.

5.3.2 Továbbfejlesztett belső átjáró irányító protokoll (EIGRP)

A RIP korlátai fejlettebb protokollok kifejlesztéséhez vezettek. A hálózati szakembereknek szükségük volt egy változó hosszúságú alhálózati maszkok használatát (VLSM) és osztályok nélküli, körzetek közötti forgalomirányítást (CIDR) támogató, nagyvállalati hálózatokban gyorsan konvergáló, könnyen bővíthető protokollra.

A Cisco kifejlesztette saját tulajdonú, speciális távolságvektor alapú protokollját, az EIGRP-t. A fejlesztések más távolságvektor alapú protokollok korlátait próbálják meg kiküszöbölni. Az EIGRP számos tulajdonságában hasonlít a RIP irányító protokollhoz, miközben sok fejlettebb funkciót is támogat.

Bár az EIGRP konfigurálása meglehetősen egyszerű, a háttérben meghúzódó tulajdonságok és opciók igen bonyolultak. Az EIGRP számos olyan tulajdonsággal rendelkezik, mely egyetlen irányító protokollban sem található meg. Mindezek a tényezők az EIGRP-t kitűnő választássá teszik a nagy, több protokollt és elsősorban Cisco eszközöket használó hálózatok esetén.



Az EIGRP két fő célja a hurokmentes irányítási környezet és a gyors konvergencia biztosítása. Ezen célok eléréséhez az EIGRP a RIP-től eltérő módszert használ a legjobb útvonal kiválasztására. Összetett mértéket használ, mely elsősorban a sávszélességen és a késleltetésen alapszik, ezáltal a célállomás felé vezető útvonal minőségének meghatározásakor az ugrásszámnál sokkal pontosabb értéket szolgáltat.

Az EIGRP által használt ún. szétszóró frissítő algoritmus (DUAL) a hurokmentes forgalomirányítást az útvonal-számítás ideje alatti működésével garantálja. A topológia megváltozásakor a DUAL egyszerre szinkronizálja az érintett forgalomirányítókat. Ezen előnyei miatt az EIGRP útvonalak adminisztratív távolsága 90, míg a RIP útvonalaké 120. A kisebb érték az EIGRP nagyobb megbízhatóságát és a mérték nagyobb pontosságát mutatja. Emiatt ha egy forgalomirányító ugyanahhoz a célhálózathoz EIGRP és RIP útvonalat is ismer, akkor az EIGRP-től származót fogja választani.

Az EIGRP a más irányító protokollok által tanult útvonalakat külső útvonalként jelöli meg. Mivel ezeknek az útvonalaknak a számításához használt információ nem annyira megbízható, mint az EIGRP mérték, ezért ezekhez az útvonalakhoz egy nagyobb adminisztratív távolságot rendel.

Az útvonal forrása	Adminisztratív távolság
Közvetlenül csatlakozó	0
Statikus	1
EIGRP összevont-útvonal	5
Külső BGP	20
Belső EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
Külső EIGRP	170
Belső BGP	200

Az EIGRP kitűnő választás bonyolult, elsősorban Cisco eszközöket használó, nagyvállalati hálózatok számára. A maximális ugrásszáma 255, amivel szintén a nagy hálózatokat támogatja. Az EIGRP több irányítótáblát is tud kezelni, amivel számos irányított protokoll (mint például az IP és az IPX) számára képes irányítási információt gyűjteni. Az EIGRP irányítótáblák, mind a helyi rendszer, mind a külső rendszer megtanult útvonalait megjelenítik.

A többi távolságvektor alapú irányító protokolltól eltérően az EIGRP nem küldi el a teljes irányítótáblájának tartalmát a frissítésekben. Csoportos küldést (multicast) alkalmazva részleges frissítést küld az adott változásokról, és nem a terület összes, csak az érintett forgalomirányítójának. Ezeket kapcsolt frissítéseknek hívják, mivel csak bizonyos paraméterekhez kapcsolódó információt tartalmaznak.

A periodikus frissítések helyett az EIGRP kis hello csomagok küldésével tartja fenn a kapcsolatot szomszédjaival. Mivel ezek kisméretűek, így mind a hello csomagok, mind a kapcsolt frissítések a sávszélességnek csak kis részét foglalják, ennek ellenére a hálózati információ folyamatos frissítése biztosított.

5.3.3 EIGRP fogalmak és táblák

Az EIGRP több táblát tart fenn a frissítési információk tárolására és a gyors konvergencia biztosításához. Az EIGRP forgalomirányítók az útvonal és a topológia információkat a RAM-ban tárolják, így gyorsan tudnak reagálni a hálózati változásokra. Három egymással összefüggő táblát tartanak fenn:

- Szomszédtábla
- Topológiatábla
- Irányítótábla

Szomszédtábla

Ez a tábla a közvetlenül kapcsolódó szomszédos forgalomirányítókról tartalmaz információt. Az EIGRP eltárolja az újonnan felfedezett szomszéd címét és a hozzá kapcsolódó interfészét.

Ha egy szomszéd egy hello csomagot küld, abban meghirdet egy megtartási időt. A megtartási idő az az idő, amíg egy forgalomirányító a szomszédját elérhetőnek tekinti. Ha a megtartási időintervallum alatt nem érkezik hello csomag a szomszédtól, akkor az időzítő lejár, a szomszéd elérhetetlennek minősül és emiatt a DUAL algoritmus újraszámolja a topológiát.

Mivel a gyors konvergencia elsősorban a szomszédokról tárolt pontos információn alapszik, ezért ez a tábla elengedhetetlen az EIGRP működéséhez.

Topológiatábla

A topológiatábla az összes EIGRP szomszédtól tanult útvonalat tartalmazza. A DUAL algoritmus a szomszéd- és topológiatáblákban található információk alapján számolja ki az egyes hálózatokhoz vezető legkisebb költségű útvonalakat.

A topológiatábla legfeljebb négy elsődleges, hurokmentes útvonalat tartalmaz célhálózatonként. Ezek a legjobb útvonalak bekerülnek az irányítótáblába is. Az EIGRP képes terheléselosztást végezni, azaz több útvonalat is használni egy adott célhoz a csomagok küldésekor. A terhelést egyenlő

költségű és nem egyenlő költségű útvonalak között is képes elosztani. Ezzel a módszerrel megelőzhető, hogy az egyes útvonalak túlterhelődjenek.

A tartalék útvonalak, más néven a második legjobb útvonalak (feasible successor) az irányítótáblában nem, csak a topológiatáblában találhatók. Ha az elsődleges útvonal kiesik, akkor a második legjobb útvonal válik a legjobb útvonallá. Ez a folyamat azonban csak akkor következik be, ha a második legjobb útvonal jelentett távolsága kisebb, mint a jelenlegi legjobb útvonal távolsága a célig.

Irányítótábla

Míg a topológiatábla számos lehetséges útvonalról tárol információt, addig az irányítótábla csak a legjobb útvonalakat tartalmazza.

Az EIGRP két módon jelenít meg információt az útvonalakról:

- Az irányítótáblában az EIGRP által tanult útvonalakat D-vel jelöli.
- A más irányító protokollok által megtanult statikus vagy dinamikus útvonalakat D EX-el jelöli, mert nem az autonóm rendszeren belüli EIGRP forgalomirányítóktól származnak.

5.3.4 EIGRP szomszédok és szomszédsági viszonyok

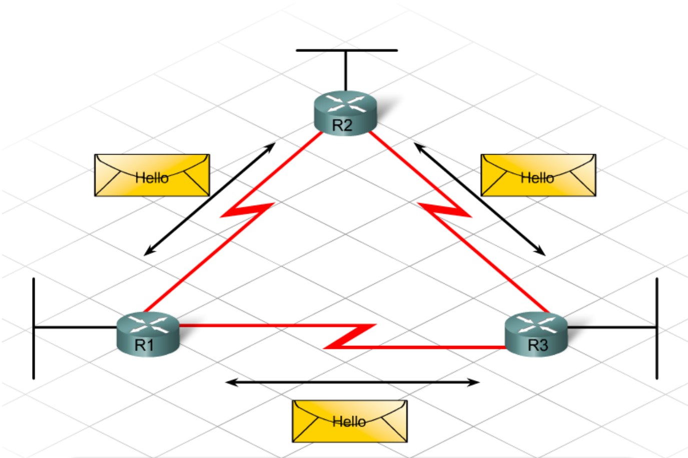
Mielőtt megkezdődhetne a forgalomirányítók közötti csomagok cseréje, fel kell fedezniük saját szomszédjaikat. Az EIGRP-szomszédok a közvetlenül kapcsolódó hálózatokon található EIGRP-t futtató forgalomirányítók.

Az EIGRP forgalomirányítók hello csomagokat küldenek a szomszédok felderítésére és a szomszédsági viszonyok kialakítására. Alapértelmezésben hello csomagokat csoportos küldés segítségével 5 másodpercenként küldenek a T1-nél gyorsabb összeköttetéseken és 60 másodpercenként a T1 vagy annál lassabb összeköttetéseken.

IP hálózat a csoportos küldés (multicast) címe 224.0.0.10. A hello csomagok a forgalomirányító interfészeiről és az interfészek címeiről tartalmaz információt. Az EIGRP forgalomirányítók feltételezik, hogy ameddig hello csomagokat kapnak a szomszédoktól, addig elérhetőek ezek a szomszédok és útvonalaik is.

A megtartási idő az az időintervallum, ameddig az EIGRP egy hello csomag megérkezésére vár. Általában a megtartási idő a hello intervallum háromszorosa. Ha a megtartási idő lejár és az EIGRP elérhetetlennek nyilvánítja az útvonalat, és a DUAL algoritmus újra kiértékeli a topológiatáblát és frissíti az irányítótáblát is.

A hello protokoll által megtanult információk a szomszédtáblába kerülnek. A sorozatszám az adott szomszédtól utoljára kapott csomag sorszámát és érkezési idejét rögzíti.



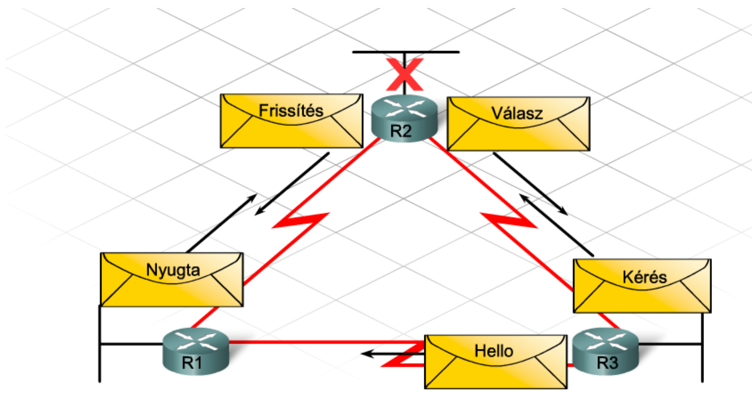
Sávszélesség	Példa a kapcsolatra	Hello intervallum	Alapértelmezett megtartási idő
1,544 Mbit/s	Többpontos Frame Relay	60 másodperc	180 másodperc
Több mint 1,544 Mbit/s	T1, Ethernet	5 másodperc	15 másodperc

A szomszédsági viszony kialakulása után az EIGRP több különböző csomagot használ az irányítótábla tartalmának frissítésére és hirdetésére. A szomszédok a következő csomagok segítségével tanulnak új -, újra felfedezett - és elérhetetlen utakat:

- Nyugtázó
- Frissítő
- Lekérdező
- Válasz

Ha egy útvonal kiesik, akkor aktív állapotba kerül és a DUAL egy új útvonalat keres a célállomáshoz. Ha talált új útvonalat, akkor az bekerül az irányítótáblába és passzív állapotba kerül.

A fent említett csomagokkal szerzett információk alapján számolja ki a DUAL algoritmus a legjobb útvonalat.



Frissítés :

- Új szomszéd felderítése esetén - egyedi címzésű (egyes küldés)
- Irányítási változás jelzése esetén - többes címzésű (többes küldés)

Nyugta:

- Adat-nélküli hello csomag egyedi címzéssel
- Megbízható adatcsomag küldésre érkező válasz: frissítés, kérés, válasz

Hello:

- A szomszédok felderítése és ellenőrzése
- Időzítők értékének a felderítése
- Csoportos (többes) küldés a 224.0.0.10 címre
- Megbízhatatlan adatküldési módszer

Kérés:

- Meghatározott információ kérése szomszédról vagy új legjobb útvonalról többes címzéssel
- Többes és egyedi címzésű is lehet

Válasz:

- Kérésre érkező válasz
- Mindig egyedi címzésű

Egy nyugtázó csomag jelzi a frissítő, a lekérdező és a válasz csomagok megérkezését. Ezek adat nélküli, kisméretű hello csomagok. Az ilyen típusú csomagok minden esetben egyedi címzéssel érkeznek.

A frissítő csomag a szomszédoknak küldött, topológia-információt tartalmazó csomag. A szomszédok ennek alapján frissítik a topológiatábláikat. Az új szomszédoknak gyakran van szükségük olyan frissítésekre, melyek az egész topológiáról tárolt információt tartalmazzák.

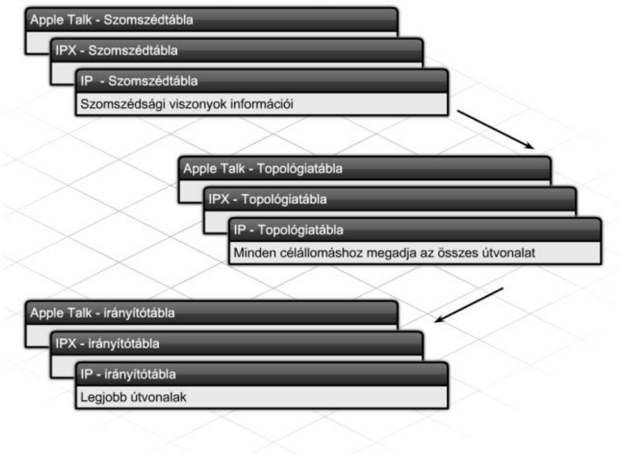
Ha a DUAL egy útvonalat aktív állapotba helyez, akkor a forgalomirányítónak lekérdező csomagot kell küldenie az összes szomszéd felé (ismernek-e a kiesett hálózathoz vezető utat). Erre a szomszédoknak választ kell küldeniük, még akkor is, ha nincs információjuk a célhálózatról. A válasz csomagokban érkező információk alapján találja meg a DUAL a legjobb útvonalat a célhálózat felé. A lekérdező csomagok egyedi küldés (unicast) és csoportos küldés (multicast) segítségével is továbbíthatók, míg a válaszok kizárólag egyedi küldéssel érkezhetnek.

Az EIGRP csomagtípusok a TCP-hez hasonló összeköttetés alapú, vagy az UDP-hez hasonló összeköttetés nélküli szolgáltatást használnak. A frissítő, a lekérdező és a válasz csomagok a TCP-hez hasonló szolgáltatást vesznek igénybe, míg a nyugtázó és a hello csomagok UDP-szerűt.

Az EIGRP a hálózati rétegtől függetlenül működő irányító protokoll. A Cisco tervezett egy saját, negyedik rétegű megbízható szállítási protokollt (Reliable Transport Protocol, RTP). Az RTP garantálja a különböző hálózati rétegbeli protokollok mindegyike számára az EIGRP csomagok kézbesítését és fogadását. Mivel bonyolult nagy hálózatok akár több hálózati rétegbeli protokollt is használhatnak, így ezen tulajdonsága alapján mondhatjuk, hogy az EIGRP rugalmas és bővíthető protokoll.

Az RTP egyaránt használható mind TCP-hez hasonló megbízható, mind UDP-hez hasonlító legjobb szándékú szállítási protokollként. Megbízható RTP esetén, a küldő fél egy nyugtát vár a fogadó féltől. A frissítő, a lekérdező és a válasz csomagok megbízható módon kerülnek kézbesítésre, míg a nyugtázó és a hello csomagok csupán legjobb szándékkal, így ezek nem igényelnek nyugtát. Az RTP egyedi küldéses és csoportos küldéses csomagot is használ. A csoportos küldéses EIGRP csomagok a fenntartott csoportos címet, a 224.0.0.10 címet használják.

Minden hálózati rétegbeli protokoll egy az adott irányító protokollért felelős protokollfüggő modulon (Protocol Dependent Module) keresztül dolgozik. Minden PDM három táblát tart karban. Egy IP-t, IPX-et, és AppleTalk-t futtató forgalomirányító például három szomszédtáblát, három topológiatáblát és három irányítótáblát kezel.



5.3.5 EIGRP mértékek és konvergencia

Az EIGRP összetett mértéket használ a célhálózathoz vezető legjobb útvonal kiválasztására, melyet a következő értékekből számol:

- Sávszélesség
- Késleltetés
- Megbízhatóság
- Terhelés

A maximális adatátviteli egység (MTU) értéket szintén tartalmazzák az irányítási frissítések, de ez nem tartozik az irányítási mértékek közé.

Az összetett mértéket számító képlet (K érték) K1-től K5-ig tartalmaz paramétereket. Alapértelmezésben K1=K3=1 és K2=K4=K5=0. Az 1 érték azt mutatja, hogy a sávszélesség és a késleltetés egyforma súllyal játszanak szerepet az összetett mérték számításában.

Sávszélesség

A sávszélesség egy állandó kbit/s-ban megadott érték. A legtöbb soros interfész az alapértelmezett 1544 kbit/s-os értéket használja. Ez a T1 kapcsolatnak megfelelő sávszélesség.

Gyakran a sávszélesség értéke nem tükrözi az adott interfész tényleges fizikai sávszélességét. A sávszélesség befolyásolja a mérték számítását, és így az EIGRP útvonalválasztását is. Ha egy 56 kbit/s-os összeköttetést 1544 kbit/s-os értékkel azonosítanak, akkor ez problémákat okozhat a konvergencia elérésében, mivel forgalomterheléssel fog küszködni.

```
R1#show int s0/0/0
Serial0/0/0 is up, line protocol is up
 Hardware is PowerQUICC Serial
Internet address is 172.16.3.1/30
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255

R1#show int s0/0/1
Serial0/0/1 is up, line protocol is up
```

```
Internet address is 192.168.10.5/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255

R1#show ip protocol
Routing Protocol is "eigrp 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
```

Az összeköttetések költségének kiszámításához használt többi mérték a késleltetés, a megbízhatóság és a terhelés.

A késleltetés a kimenő interfész típusától függő állandó érték. Az alapértelmezett érték 20,000 mikroszekundum soros interfészek, és 100 mikroszekundum Fast Ethernet interfészek esetén.

A késleltetés nem a csomagok célállomáshoz történő megérkezéséhez szükséges időt mutatja. A késleltetési érték megváltoztatása az adott interfészeken ténylegesen nem befolyásolja a hálózat működését.

A megbízhatóság megadja, hogy milyen gyakran történik hiba az adott összeköttetésen. A késleltetéstől eltérően ez az érték automatikusan változik az összeköttetés körülményeitől függően. Az értékek 0 és 255 között lehetnek. A 255/255 –ös érték 100%-os megbízhatóságot jelent.

A terhelés az összeköttetést használó forgalom nagyságát jelöli. Egy kisebb terhelési érték jobb értéket jelent, mint a nagy. Az 1/255 jelentené például a minimálisan terhelt, míg a 255/255 a 100%-osan kihasznált összeköttetést.

Átviteli közeg	Késleltetés
100M ATM	100 μS
Fast Ethernet	100 μS
FDDI	100 μS
IHSSI	20,000 μS
16M Token Ring	630 μS
Ethernet	1000 μS
T1(Serial Default)	20,000 μS
512 K	20,000 μS
DS0	20,000 μS
56 K	20,000 μS
Belső BGP	200 μS

Megjegyzés: μS=mikroszekundum

Az EIGRP topológiatábla szolgál a legkisebb távolság (Feaseable Distance, FD) és a meghirdetett távolság (Advertized, AD), vagy a jelentett távolság (Reported, RD) mértékekhez tartozó értékek karbantartására. A DUAL ezen értékek alapján választja ki a legjobb - és a második legjobb útvonalat.

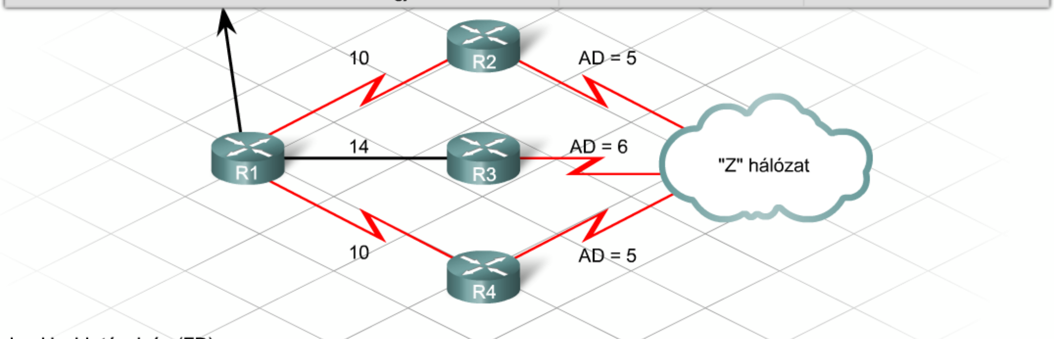
A legkisebb távolság a legjobb EIGRP mérték a forgalomirányítótól a célhálózatig.

A meghirdetett távolság a szomszéd által hirdetett legjobb mérték.

A legkisebb távolsággal rendelkező hurokmentes útvonal lesz a legjobb útvonal. Az aktuális topológiától függően egy adott célállomásig több legjobb útvonal is létezhet. A második legjobb útvonal a legjobb útvonal legkisebb távolságánál kisebb jelentett távolsággal rendelkező útvonal lesz.

A DUAL a topológia-változás után gyors konvergenciát tesz lehetővé. A második legjobb útvonalakat a topológiatáblában tárolja és a legjobbat közülük az eredeti legjobb útvonal kiesése esetén legjobb útvonalként az irányítótáblába helyezi. Ha nem létezik második legjobb útvonal, akkor az eredeti legjobb útvonal aktív állapotba kerül és lekérdező csomagok küldése következik az új legjobb útvonal megtalálása érdekében.

	Legkisebb távolság	Hirdetett távolság
A "Z" hálózatba az R2-ön keresztül vezet a legjobb útvonal	FD = 15	AD = 5
A "Z" hálózatba az R3-on keresztül vezet a második legjobb útvonal	FD = 20	AD = 6
A "Z" hálózatba az R4-en keresztül vezet a legjobb útvonal	FD = 15	AD = 5



Legkisebb távolság (FD)
A forgalomirányítótól a célhálózatig terjedő útvonal minimális távolsága (mértéke).

Hirdetett távolság (AD) vagy Jelentett távolság(RD):
A célállomás felé vezető útvonalon lévő szomszédos forgalomirányító által hirdetett távolság (mérték). *A szomszédos forgalomirányító távolsága*

További információ

Egy EIGRP irányítótábla bejegyzésben a "via" szócska megelőzi a legjobb útvonal, következő ugrás címét. A legkisebb távolság az adminisztratív távolság után megjelenő mérték. Az alábbi bejegyzésben, a 192.168.1.0/24 hálózatba vezető legjobb útvonal következő ugrásának címe 192.168.10.10, és a legkisebb távolság 3014400:

D 192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:00:31, Serial0/0/1

5.4 EIGRP megvalósítása

5.4.1 EIGRP konfigurálása

EIGRP-t alapszinten nagyon egyszerű konfigurálni. Sok hasonlóságot mutat a RIPv2-vel.

Az EIGRP irányítási folyamatának elindításához alkalmazza a következő két lépést:

1. lépés

Az EIGRP irányítási folyamat engedélyezése.

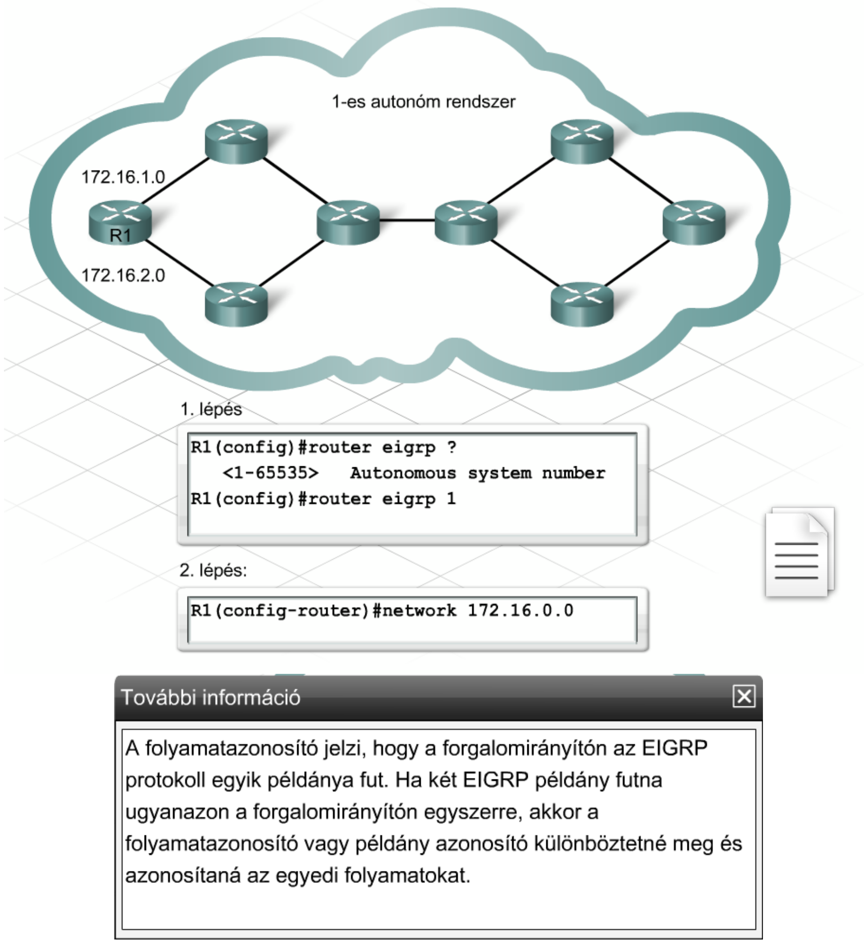
Az EIGRP irányítási folyamat engedélyezéséhez egy autonóm rendszerazonosító (autonomous system - AS) szükséges. Ez az autonóm rendszerazonosító bármilyen 16 bites érték lehet, és egy vállalat vagy szervezet forgalomirányítóit azonosítja. Bár az EIGRP ezt az értéket autonóm rendszerazonosítónak hívja, valójában folyamatazonosítóként szolgál. Ennek az AS azonosítónak csak helyi jelentősége van és nem azonos az Internet Assigned Numbers Authority (IANA) által kiosztott autonóm rendszer számával.

Az AS számnak az adott EIGRP irányítási folyamatban résztvevő forgalomirányítók mindegyikén egyeznie kell.

2. lépés

A network parancs kiadása minden hirdetendő hálózatra.

A `network` parancs határozza meg az EIGRP számára az irányítási folyamatban résztvevő interfészeket és hálózatokat.



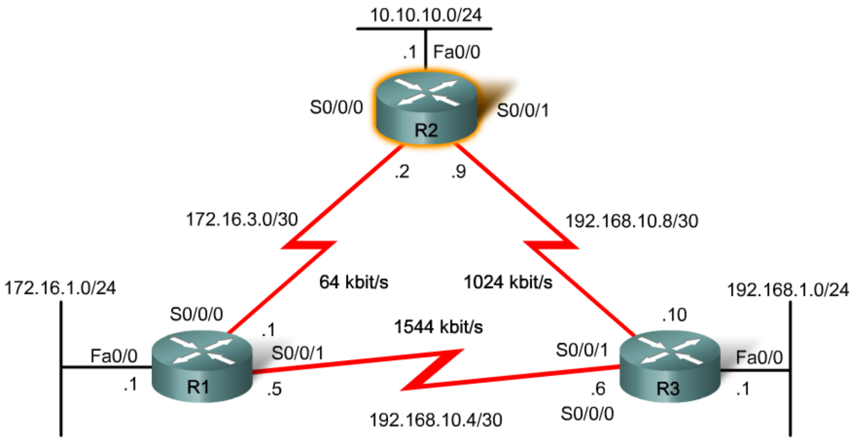
Csak bizonyos alhálózatok hirdetése esetén kell megadni a helyettesítő maszkot a hálózat címe után. A helyettesítő maszk kiszámításához vonja ki az alhálózati maszkot a 255.255.255.255-ből.

A Cisco IOS bizonyos verziói lehetővé teszik a helyettesítő maszk helyett az alhálózati maszk használatát. Még akkor is, ha az alhálózati maszkot használjuk, a `show running-config` parancs a helyettesítő maszkot jeleníti meg.

További két parancs egészíti ki az EIGRP tipikus alapszintű konfigurációját.

A szomszédsági viszonyok változásainak követéseihez adja hozzá az `eigrp log-neighbor-changes` parancsot a konfigurációhoz! Ez elősegíti az EIGRP hálózat stabilitásának megfigyelését a hálózati rendszergazda számára.

Olyan soros összeköttetéseken, ahol a sávszélesség nem az alapértelmezett 1,544 Mbit/s, adja ki a `Bandwith` parancsot az összeköttetés tényleges sebességének kbit/s-ban megadott értékével. A nem pontos sávszélesség érték megakadályozhatja a ténylegesen legjobb útvonal kiválasztását.



Az EIGRP engedélyezése után, bármely EIGRP-vel és megfelelő AS azonosítóval konfigurált forgalomirányító beléphet az EIGRP hálózatba. A különböző és ellentmondásos útvonal információval rendelkező forgalomirányítók befolyásolhatják, illetve helytelen információval tölthetik meg az irányítótáblát. Ennek megelőzésére lehetőség van az EIGRP konfiguráción belül a hirdetések hitelesítésének engedélyezésére. Amint a szomszédok hitelesítése engedélyezett, a forgalomirányító a frissítések forrásait az információk feldolgozása előtt hitelesíti.

Az EIGRP hitelesítéséhez előre megosztott kulcsokra van szükség. Az EIGRP kulcsokat a rendszergazda tartja karban egy kulcsláncon keresztül. Az EIGRP hitelesítések konfigurációja két lépésből áll: a kulcs létrehozása és a kulcsot használó hitelesítés engedélyezése.

Kulcs létrehozása

A kulcs létrehozásához a következő parancsokra van szükség:

`key chain` *`lánc_neve`*

- Globális konfigurációs parancs.
- A kulcslánc nevét határozza meg és belép kulcslánc konfigurációs módba.

`key` *`kulcs_azonosító`*

- Azonosítja a kulcs számát és belép a megadott kulcsazonosító konfigurációs módba.

`key-string` *`szöveg`*

- Azonosítja a kulcs karakterláncot vagy más néven jelszót. Ennek minden EIGRP forgalomirányítón egyeznie kell.

Hitelesítés engedélyezése

Az EIGRP MD5 hitelesítését a kulcs segítségével a következő interfész konfigurációs parancsokkal lehet engedélyezni:

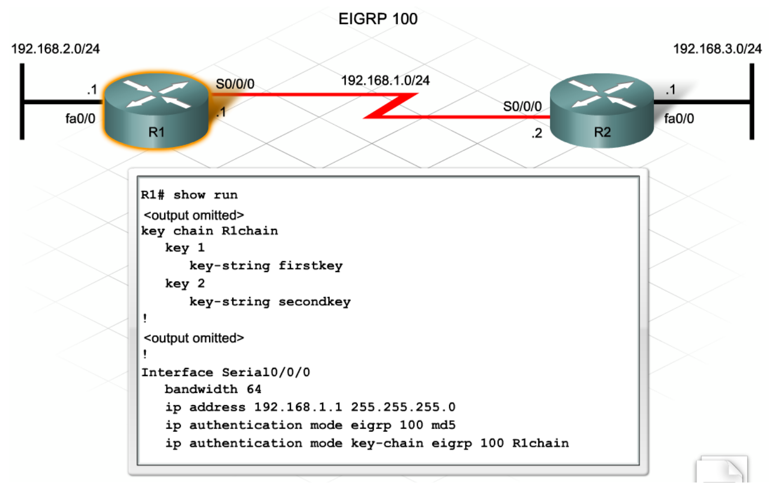
`ip authentication mode eigrp md5`

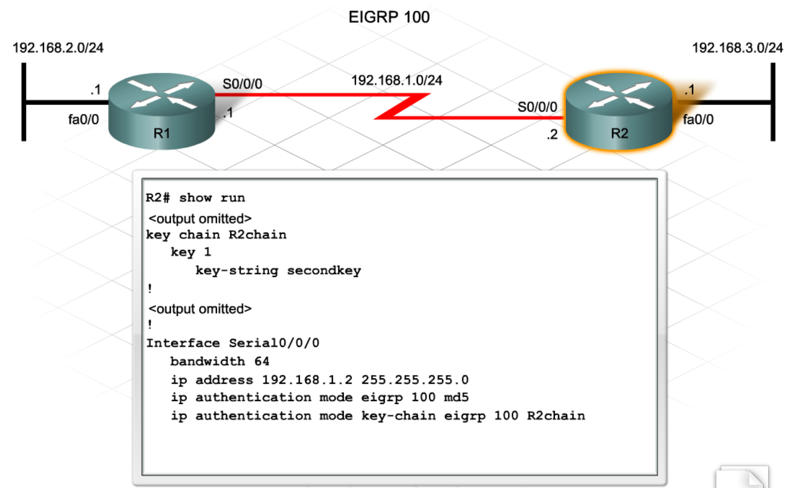
- Meghatározza, hogy MD5 hitelesítés szükséges a csomagok küldéséhez, fogadásához.

`ip authentication key-chain eigrp` *`AS lánc_neve`*

- Az AS határozza meg az EIGRP konfiguráció AS azonosítóját.

A lánc_neve paraméter határozza meg az előzőleg konfigurált kulcsláncot.





További információ

Választható paraméterek konfigurálhatók a kulcslánc részeként. Ilyen választható paraméterek közé tartozik a kulcs létrehozásának dátuma, a kulcs élettartama, valamint a kulcs használatának végső dátuma. A választható paraméterek konfigurálásához kulcs-konfigurációs módba kell lépni.

`accept-lifetime` *`start-time {infinite | end-time | duration seconds}`*

- Meghatározza, mikor fogadták el a kulcsot érkező csomagok esetén!
- A kezdő idő általában **óó:pp:mm hónap nap év** formátumban jelenik meg.

`send-lifetime` *`start-time {infinite | end-time | duration seconds}`*

- Meghatározza, mikor használható a kulcs küldött csomagok esetén!

5.4.2 EIGRP útvonal összevonás

A RIP-hez hasonlóan az EIGRP osztály alapú határokon szintén automatikusan összevonja az alhálózatokra bontott hálózatokat. Az EIGRP összesen egy bejegyzést készít az irányítótáblájában az összevont útvonal számára. A legjobb útvonal ez esetben mindig az összevont útvonal, így minden olyan forgalom, melyet az alhálózatokba címeztek ezen az egy útvonalon megy végig.

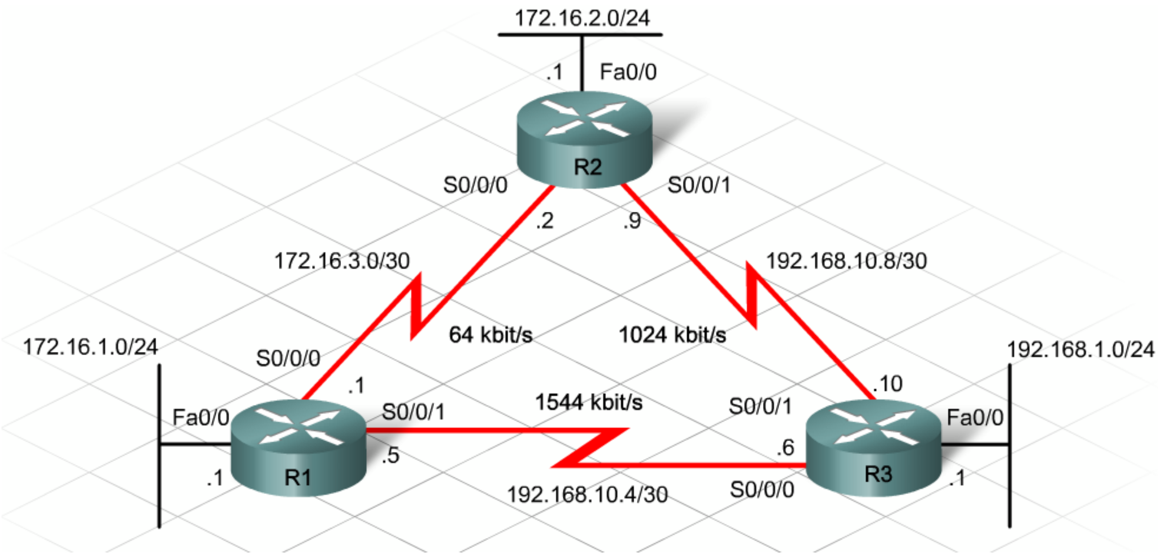
Nagyvállalati hálózatokban az összevont útvonal nem feltétlenül a legjobb választás az egyes alhálózatokba címzett csomagok számára. Az egyetlen megoldás, mellyel a forgalomirányítók megtalálhatják az alhálózatokhoz vezető legjobb útvonalaikat az, hogyha alhálózati információt is küldenek a szomszédok.

Ha az alapértelmezett összegzés tiltva van, akkor a frissítések tartalmazzák az alhálózati információt. Az irányítótáblába minden egyes alhálózathoz bekerül egy bejegyzés, valamint egy másik bejegyzés az összevont útvonal számára. Az összevont útvonalat szülő útvonalaknak, míg az alhálózati bejegyzéseket gyermek útvonalaknak nevezzük.

Az EIGRP minden szülő-útvonalra vonatkozóan egy Null0 összevont útvonalat helyez el az irányítótáblába. A Null0 interfész jelzi, hogy nem egy tényleges útvonalról van szó, hanem csak egy hirdetési célra használt összevont útvonalról. Ha egy csomag célcíme azonos valamely gyermek útvonallal, akkor a forgalomirányító a megfelelő interfészen továbbítja azt. Ha a csomag célcíme egyetlen gyermek útvonallal sem, de az összevont útvonallal egyezik, akkor a csomagot eldobja a forgalomirányító.

Az alapértelmezett összevonás használata kisebb irányítótáblákat, míg az összevonás letiltása nagyobb méretű frissítéseket és nagy táblákat eredményez. A teljes hálózati teljesítmény és forgalomminták határozzák meg, hogy az automatikus összevonás előnyös-e.

A `no auto-summary` parancs segítségével kikapcsolható az alapértelmezett összevonás.



```
R1#show ip route
 (**output omitted**)

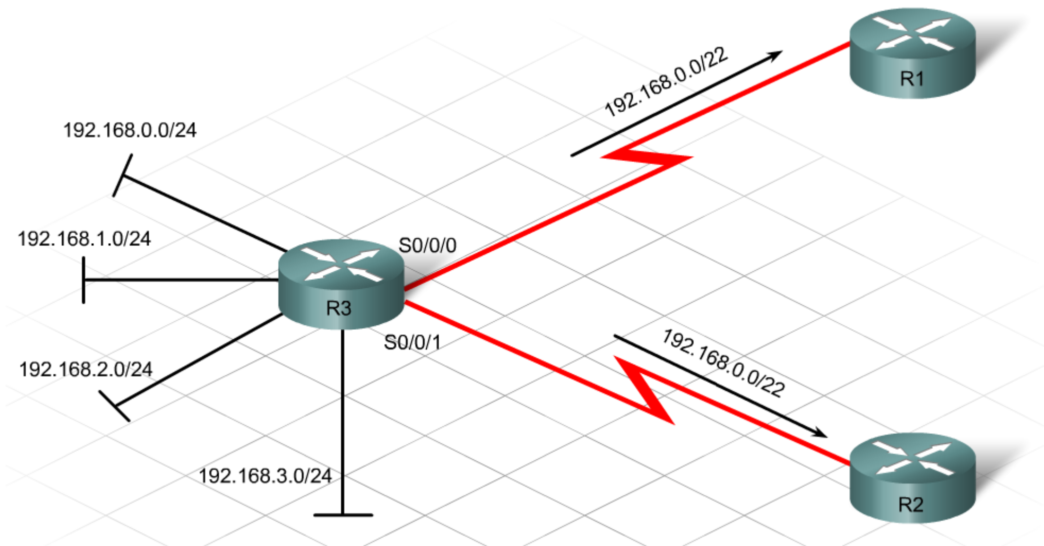
Gateway of last resort is not set
   192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:45:09, Null0
C       192.168.10.4/30 is directly connected, Serial0/0/1
S       192.168.10.8/30 [90/3523840] via 192.168.10.6, 00:44:56, Serial0/0/1
   172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 00:46:10, Null0
C       172.16.1.0/24 is directly connected, FastEthernet0/0
D       172.16.2.0/24 [90/40514560] via 172.16.3.2, 00:45:09, Serial0/0/0
C       172.16.3.0/24 is directly connected, Serial0/0/0
D    192.168.1.0/24 [90/2172416] via 192.168.10.6, 00:44:55, Serial0/0/1
```

Kikapcsolt automatikus összevonás mellett minden alhálózatot hirdetnek a forgalomirányítók. Egy rendszergazda találkozhat olyan esettel, amikor bizonyos útvonalakat összegezni kell, míg másokat nem. A döntés az alhálózatok elhelyezkedésétől is függ. Négy ugyanahhoz a forgalomirányítóhoz kapcsolódó folytonos alhálózat esetében például érdemes összevonni.

A manuális útvonal összevonás az EIGRP útvonalak pontosabb ellenőrzését teszi lehetővé, így a rendszergazda döntheti el, hogy mely interfészek mely alhálózatait hirdeti összevont útvonalként.

A manuális összevonást interfészenként kell elvégezni. Ez az eljárás a rendszergazda számára teljes ellenőrzést biztosít. Egy manuálisan összevont útvonal az irányítótáblában logikai (nem fizikai) interfésztől származó EIGRP útvonalként jelenik meg:

```
D 192.168.0.0/22 is a summary, Null0
```



22 egyező bit megfelel a /22-es vagy 255.255.252.0 alhálózati maszknak

```
R3(config)#interface serial 0/0/0
R3(config-if)#ip summary-address eigrp 1 192.168.0.0 255.255.252.0
R3(config-if)#interface serial 0/0/1
R3(config-if)#ip summary-address eigrp 1 192.168.0.0 255.255.252.0
```

Bár az EIGRP viszonylag egyszerűen konfigurálható protokoll, kifinomult technológiákat használ a távolságvektor alapú irányító protokoll korlátainak kiküszöbölésére. Fontos, hogy megértsük ezeket a technológiákat, hogy megfelelően tudjuk egy EIGRP hálózat konfigurációját ellenőrizni és a hibákat megkeresni. Néhány ellenőrzésre szolgáló parancs:

`show ip protocols`

- Megmutatja, hogy az EIGRP a megfelelő hálózatokat hirdeti-e,
- valamint kimenetéből leolvasható az autonóm rendszerazonosító és az adminisztratív

`show ip route`

- Segítségével leellenőrizhető, hogy minden EIGRP útvonal az irányítótáblában van-e.
- Az EIGRP útvonalak **D** vagy **D EX** betűkkel vannak megjelölve,
- és a belső utak alapértelmezett adminisztratív távolsága 90.

`show ip eigrp neighbors detail`

- Segítségével leellenőrizhetők az EIGRP szomszédsági viszonyai.
- Megmutatja a szomszédos forgalomirányítók interfészeit és IP-címeit.

`show ip eigrp topology`

- Megmutatja a legjobb és az összes második legjobb útvonalat,
- valamint a legkisebb és a jelentett távolságot.

`show ip eigrp interfaces detail`

- Segítségével leellenőrizhetők az EIGRP-t használó interfészek.

`show ip eigrp traffic`

- Megmutatja az EIGRP által küldött és fogadott csomagok típusát és számát.

Ezeknek a parancsoknak az elsődleges célja az EIGRP szomszédsági viszonyok sikeres létrejöttének, valamint a forgalomirányítók közötti sikeres információcserének az ellenőrzése. Az EIGRP a szomszédsági viszonyok kialakulása nélkül nem működhet, így minden más hiba felderítése előtt ennek az ellenőrzésére van szükség.

Ha a szomszédsági viszonyok megfelelőek, de továbbra is fennáll a probléma, akkor a rendszergazdának a debug parancsok segítségével kell a hibákat megkeresnie. Ezek a parancsok lehetővé teszik az EIGRP események valós-idejű nyomonkövetését.

`debug eigrp packet`

- megmutatja az összes EIGRP csomag küldését és fogadását

`debug eigrp fsm`

- megjeleníti az EIGRP-nek a második legjobb útvonalakkal kapcsolatos tevékenységeit, aminek alapján megállapítható, hogy az útvonalakat törölték, felfedezték vagy bejegyezték-e.

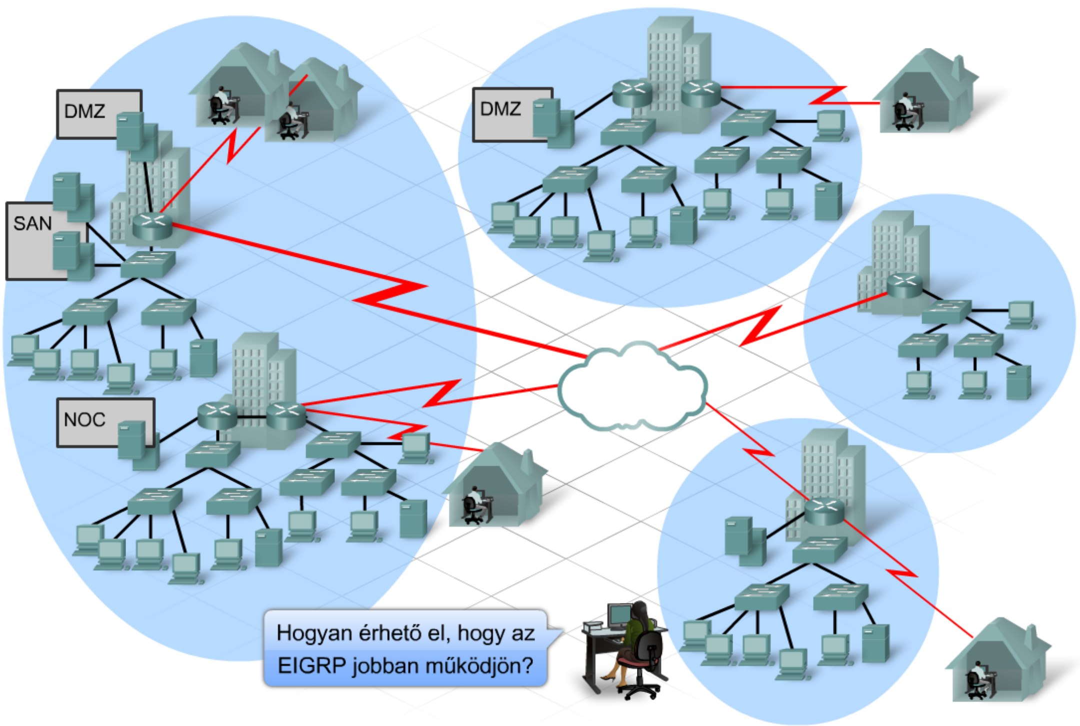
A debug folyamatok nagy sávszélességet és feldolgozási időt vesznek igénybe, különösen akkor, ha az EIGRP-hez hasonló nagyon komplex protokoll monitorozásáról van szó. Ezek a parancsok olyan részleteket nyújtanak, amelyek segítségével pontosan meghatározható egy elveszett EIGRP útvonal forrása, vagy egy hiányzó szomszédsági viszony. Természetesen ezen parancsok használata leronthatja a hálózati teljesítményt.

5.4.4 Az EIGRP korlátai és problémái

Bár az EIGRP egy erőteljes és kifinomult irányító protokoll, számos tényező korlátozhatja a használatát:

- Nem működik több gyártó eszközével kialakított rendszerben, mivel Cisco tulajdonú protokoll.
- Legjobban nem hierarchikus hálózati felépítés mellett működik.
- Minden forgalomirányítónak ugyanazzal az autonóm rendszerazonosítóval kell rendelkeznie, vagyis tovább nem csoportosíthatók az eszközök.
- Hatására létrejöhetnek hatalmas irányítótáblák, melyek sok frissítést eredményeznek és nagy sávszélesség használatot vonnak maguk után.
- Több memóriát és feldolgozást igényel, mint a RIP
- Alapértelmezett beállításaival nem működik hatékonyan
- A rendszergazdának magas szintű technikai tudással kell rendelkeznie, mind a protokollal, mind a hálózattal kapcsolatban.

Az EIGRP a legjobb távolságvektor alapú irányító protokoll, mely tipikusan kapcsolatállapot alapú irányító protokollokra jellemző tulajdonságokat is magába foglal (kapcsolt frissítések, szomszédsági viszonyok). Az EIGRP számos tulajdonságának sikeres használata figyelmes konfigurálást, felügyeletet és hibafelderítést igényel.



5.5 A fejezet összefoglalása

- A nagyvállalati hálózatok hierarchikus felépítésűek az információáramlás megkönnyítése érdekében.
- Különböző topológiák léteznek a nagyvállalati hálózatokban, ide tartoznak a csillag, kiterjesztett csillag és háló topológiák.
- A hálózatok általában statikus és dinamikus forgalomirányítást is használnak az adatok továbbításához.
- A statikus útvonalakat manuálisan kell konfigurálni, növelik a hálózat biztonságát és csökkentik a forgalomirányítók terhelését.
- A dinamikus útvonalakat a forgalomirányítók irányító protokollokon keresztül tanulják meg és a célállomáshoz vezető útvonalak kiszámítása automatikusan történik.
- Az alapértelmezett útvonal olyan információ továbbítására alkalmas, melyhez nem található bejegyzés az irányítótáblában.
- A dinamikus irányító protokollokat két osztályba soroljuk: léteznek távolságvektor alapú és kapcsolatállapot alapú irányító protokollok.
- A RIP egy távolságvektor alapú irányító protokoll.
- A RIPv1 az egész irányítótábláját, szórásos üzenetben, 30 másodpercenként továbbítja a csatlakozó forgalomirányítóknak.
- A RIPv2 többes-küldést alkalmazva osztja meg az irányítótábla tartalmát.
- A RIP irányító protokollt nagyon egyszerű konfigurálni és karbantartani, de nem skálázható jól és lassan konvergál.
- A távolságvektor alapú irányító protokollok hajlamosak az irányítási hurkok kialakítására.
- Az EIGRP egy Cisco tulajdonú távolságvektor alapú irányító protokoll számos továbbfejlesztett tulajdonsággal.
- Gyorsan konvergál és összetett mértéket használ a megbízhatóbb irányítási információk érdekében.
- Az EIGRP csak kötött frissítéseket küld többes küldéssel, így kisebb a sávszélességigénye.
- A RIPv2 többes küldéssel a 224.0.0.9 címre küldi 30 másodpercenként az irányítótáblájának tartalmát.
- Az irányítási hurkok kialakulását a szétszóró frissítő algoritmus (DUAL) használata akadályozza meg.
- Az EIGRP több csomagtípust használ a szomszéd-, a topológia- és az irányítótáblák karbantartására.
- Az EIGRP a legjobb és a második legjobb útvonalakról is karbantart információt az esetleges meghibásodások esetén a gyors konvergencia eléréséhez.
- Az EIGRP autonóm rendszer azonosítót használ, amik tulajdonképpen folyamatazonosítók.
- Egyenlő és különböző terhelésű útvonalak közötti terheléselosztást is támogat.
- Az EIGRP automatikus útvonal összevonást végez, mely kikapcsolható és az irányítás könnyebb ellenőrzése érdekében manuálisan is elvégezhető.
- Az EIGRP-t egyszerű konfigurálni, de nehéz karbantartani és optimizálni.

6. Kapcsolatállapot alapú forgalomirányítás

6.1 OSPF protokollal történő forgalomirányítás

6.1.1 Kapcsolatállapot alapú protokoll működése

A vállalati hálózatok és az internetszolgáltatók a hierarchikus (egymásra épülő részekből álló) felépítésük és bővíthetőségük miatt kapcsolatállapot alapú forgalomirányító protokollt alkalmaznak. A távolságvektor alapú forgalomirányító protokollok általában nem alkalmasak összetett vállalati hálózatok forgalomirányítására.

Kapcsolatállapot alapú protokollra példa a Legrövidebb út protokoll (OSPF - Open Shortest Path First,), amely az Internet mérnöki munkacsoport (IETF - Internet Engineering Task Force) által kifejlesztett nyílt szabványú, IP feletti irányító protokoll.

Az OSPF osztály nélküli belső átjáró protokoll (IGP - interior gateway protocol), amely a bővithetőség érdekében a hálózatot különálló részekre, un. területekre (area) bontja. A hálózati szakember számára a több terület alkalmazása lehetőséget ad meghatározott útvonalak összevonására és bizonyos irányítási feladatok egyetlen területre történő leszűkítésére.

A kapcsolatállapot alapú irányító protokollok, mint például az OSPF, nem küldik el egész irányítótáblájukat rendszeres időközönként. Ehelyett a hálózat konvergálása (közelítése az optimális működéshez) után kizárólag a topológia megváltozása (például egy kapcsolat megszakadása) következtében küldenek frissítéseket. Az OSPF teljes körű frissítést csupán 30 percenként küld.

A kapcsolatállapot alapú irányító protokollok, mint az OSPF is, kiválóan alkalmazhatók nagyobb, hierarchikus hálózatokban, ahol a gyors konvergencia fontos.

A kapcsolatállapot alapú irányító protokollok a távolságvektor alapúval összehasonlítva:

- összetett hálózattervezést és konfigurációt igényel
- nagyobb az erőforrásigénye
- több táblázat karbantartása miatt nagyobb memóriát igényel
- az összetett irányítási számítások következtében nagyobb a CPU- és a feldolgozásigénye

Ezen követelmények nem jelentenek akadályt, hiszen napjainkban nagy teljesítményű forgalomirányítók állnak rendelkezésre.

RIP protokollt alkalmazó forgalomirányítók a közvetlen szomszédjaikról kapnak frissítéseket, de a hálózat egészéről nincsenek ismereteik. Az OSPF protokollt futtató forgalomirányítók viszont létrehozzák a teljes hálózaton belül saját területük térképét, és ez által képesek gyorsan meghatározni új, hurokmentes útvonalakat egy kapcsolat megszakadása (hálózati ad atcsatorna hibája) esetén.

Az OSPF nem összegzi automatikusan az útvonalakat a főbb hálózathatárokon, továbbá a Cisco OSPF implementációja figyelembe veszi a sávszélességet egy kapcsolat költségének meghatározásánál. A „legjobb útvonal” meghatározásához költségmértéket alkalmaz. A Cisco OSPF implementációja egy útvonal költségének meghatározásánál a sávszélességet veszi figyelembe. A nagyobb sávszélességű összeköttetés kisebb költséget jelent. A célhoz vezető legkisebb költségű útvonal lesz a legmegfelelőbb.

A legjobb út meghatározásánál a forgalomirányító számára a sávszélesség alapú mérték megbízhatóbb, az ugrásszám alapúnál. A mérték megbízhatóságából és pontosságából adódóan az OSPF adminisztratív távolsága 110, mely kisebb a RIP protokollénál.

6.1.2 OSPF mérték és konvergencia

Az OSPF protokoll a kapcsolat költségmértékét, annak sávszélességére vagy sebességére alapozza. Meghatározott célhálózatba vezető útvonal költsége az egyes összeköttetések költségének összegéből adódik. Egy hálózatba vezető összes útvonal közül a legkisebb összköltségű útvonal részesül előnyben és kerül az irányítótáblába.

A költség kiszámítása az alábbi képlet alapján történik:

Költség = 100.000.000 / az összeköttetés sávszélessége [bit/s]

A számítás alapjául az interfészen beállított sávszélesség szolgál, amely a `show interfaces` parancs segítségével tekinthető meg.

A képlet alkalmazása során problémát eredményeznek a 100 Mbit/s vagy nagyobb sebességű kapcsolatok, mint a Fast és Gigabit Ethernet. Tekintet nélkül e két összeköttetés sebességének különbségére, mindkét esetben a költségérték 1, így különbözőségük ellenére azonos eredményt nyújtanak. Ennek ellensúlyozása érdekében, az `ip ospf cost` parancs alkalmazásával az interfész költsége kézzel beállítható.

Az interfész típusa	10^8/bit/s = költség
Fast Ethernet és gyorsabb	10^8/100,000,000 bit/s = 1
Ethernet	10^8/10,000,000 bit/s = 10
E1	10^8/2,048,000 bit/s = 48
T1	10^8/1,544,000 bit/s = 64
128 kbit/s	10^8/128,000 bit/s = 781
64 kbit/s	10^8/64,000 bit/s = 1562
56 kbit/s	10^8/56,000 bit/s = 1785

Az azonos területhez tartozó OSPF forgalomirányítók a kapcsolat-állapotukról ún. kapcsolatállapot-hirdetéseket (LSA – Link State Advertisement) küldenek a szomszédjaiknak.

Miután egy OSPF forgalomirányító LSA üzenetek segítségével a teljes terület minden összeköttetését feltérképezi azaz meghatározza a terület hálózat térképét, ebből az SPF algoritmus vagy más néven Dijkstra algoritmus alkalmazásával felépít egy az adott forgalomirányitóból kiinduló területi topológia fát. Minden forgalomirányító, mely az algoritmust futtatja, az SPF fa gyökerében saját magát tünteti fel. A gyökérből kiindulva, az összköltség alapján minden célhálózathoz meghatározza a legrövidebb utat. Ezek összessége az SPF fa.

Az OSPF kapcsolatállapot vagy topológiai adatbázis tárolja az SPF fa információit, és minden hálózathoz vezető legrövidebb útvonal bekerül az irányítótáblába.

A konvergencia bekövetkezik, ha minden forgalomirányító:

- Megkapott minden információt a hálózat összes irányáról
- Az ismereteket feldolgozta az SPF algoritmus alkalmazásával
- Frissítette az irányítótábláját

6.1.3 OSPF szomszédok és szomszédsági viszony

OSPF esetén a kapcsolatállapot frissítéseket változások esetén küldik ki a forgalomirányítók. De vajon honnan értesül egy forgalomirányító szomszédja kieséséről? Az OSPF forgalomirányítók szomszédsági kapcsolatokat építenek ki és tartanak fenn más csatlakozó forgalomirányítókkal. A szomszédokkal kialakított legteljesebb állapot a szomszédsági viszony, melynek során két forgalomirányító egymással irányítási információkat cserél. A szomszédsági viszony kialakítását követően a két forgalomirányító elkezdi a kapcsolatállapot frissítések küldését egymásnak. A teljes értékű (full state) szomszédsági viszonyt akkor érik el, ha kapcsolatállapot-adatbázisuk már összhangban van egymással.

A teljes értékű szomszédsági viszony kialakítása során, a forgalomirányítók az alábbi állapotokon haladnak keresztül:

- Kezdeti
- Két-utas
- Kezdés utáni
- Adat cserélő
- Adat feltöltő
- Teljes értékű

A szomszédsági kapcsolatok kialakítása a Hello protokollra épül, melynek során a közvetlenül kapcsolódó OSPF forgalomirányítók kisméretű csomagokat küldenek egymásnak a 224.0.0.5 csoportos (többes küldéses, multicast) cím alkalmazásával. A Hello üzenetek küldése Ethernet és üzenetszórásos hálózatokon 10, míg nem szórásos hálózatokon 30 másodpercenként történik. A forgalomirányítók beállításaiban a hello időzítő, a várakozási időzítő, a hálózattípus, a hitelesítés típusa és a hitelesítési adatok egyaránt megváltoztathatók. Szomszédsági viszony esetén ezeknek a paramétereknek egyezniük kell. A forgalomirányítók e viszonyokat a kapcsolatállapot adatbázisban tárolják.

Kezdeti A forgalomirányító egy kezdeti hello csomagot kap a szomszédjától. Amikor ez megtörténik, a saját hello csomagjába, mint nyugtába, beleteszi a küldő forgalomirányító azonosítóját.
Két-utas Ha két forgalomirányító látja egymás azonosítóját a hello csomagokban, két-irányú kommunikáció kezdődik köztük. A forgalomirányító ebbe az állapotba kerül, ha egy beérkező hello csomag szomszédsági mezőjében saját azonosítóját látja. Ekkor eldönti, hogy kialakítson-e teljes értékű szomszédsági viszonyt.
Kezdés utáni A forgalomirányítók egy "mester-szolga" kapcsolatot alakítanak ki és megválasztják a szomszédsági viszony felépítésének kezdő sorszámát. A két forgalomirányító közül a nagyobb azonosítóval rendelkező lesz a mester és megkezdi az adatcserét.
Adat cserélő Az OSPF forgalomirányítók adatbázis leíró (DBD - database descriptor) csomagokat cserélnek, melyek csupán LSA fejrészeket tartalmaznak. A DBD leírja a tejes kapcsolatállapot adatbázis tartalmát. Minden DBD csomag sorszámmal rendelkezik, melyet kizárólag a mester forgalomirányító növelhet.
Adat feltöltő A DBD csomagokból nyert adatok alapján a forgalomirányítók kapcsolatállapot kérelmet küldenek specifikusabb adatokért. A szomszéd a kért kapcsolatállapot adatokat kapcsolatállapot frissítésekben küldi el.
Teljes értékű Az összes forgalomirányító és hálózat LSA cseréje megtörtént és a forgalomirányítók adatbázisa teljes mértékben összehangolt.

Az OSPF forgalomirányító normál esetben teljes értékű szomszédsági állapotban van. Ha az eszköz huzamosabb ideig egy másik állapotban marad, akkor valamilyen problémára lehet következtetni. Ilyen problémát okozhatnak például a nem megegyező beállítások. Az egyetlen kivételt a kétutas állapot képezi. Szórásos környezetben egy forgalomirányító a kijelölt forgalomirányítóval (DR - designated router) és a tartalék kijelölt forgalomirányítóval (BDR - backup designated router) alakít ki teljes értékű szomszédsági viszonyt.

A DR és a BDR forgalomirányítók megválasztásával a frissítések száma és a szükségtelen forgalom csökkenthető, továbbá a forgalomirányítók feldolgozási folyamata gyorsítható. Ennek megvalósításához egyedül az szükséges, hogy a forgalomirányítók csak a kijelölt forgalomirányítótól fogadjanak frissítéseket. Szórásos hálózati szegmensen egyetlen kijelölt, illetve tartalék kijelölt forgalomirányító jelenléte szükséges, az összes többi forgalomirányító csak ezekkel van szomszédsági kapcsolatban. Egy kapcsolat kiesésekor, az a forgalomirányító, amelyiknek érzékeli a kapcsolat megszünését, üzenetet küld a DR forgalomirányítónak a 224.0.0.6 csoportos címet használva. A DR felelőssége eljuttatni az információt a többi OSPF forgalomirányítónak a 224.0.0.5 csoportos cím alkalmazásával. Azon kívül, hogy így csökkenthető a frissítések száma, a folyamat biztosítja, hogy minden forgalomirányító egységesen, egyidőben és ugyanazt az információt kapja meg egyetlen forrásból.

A tartalék kijelölt forgalomirányító (BDR) jelenlétével kiküszöbölhető a hálózat egyetlen hibapontból származó sérülékenysége. A kijelölt forgalomirányítóhoz hasonlóan a BDR is figyeli a 224.0.0.6 IP-címre érkező üzeneteket, illetve megkapja a frissítéseket. A DR működésképtelenné válása esetén a BDR forgalomirányító azonnal átveszi a kijelölt forgalomirányító szerepét, és új BDR választás történik a szegmensen. A kitüntetett szereppel nem rendelkező forgalomirányítók neve: DROther.

Helyi hálózatokon a legmagasabb OSPF forgalomirányító azonosítóval rendelkező forgalomirányítót lesz a DR. A második legnagyobb forgalomirányító-azonosítóval rendelkező lesz a BDR.

1. A forgalomirányító azonosító egy IP-cím, amelyet az alábbi paraméterek befolyásolnak:
1. A `router-id` parancs alkalmazásával meghatározott érték
2. Ha nincs beállított érték a legmagasabb beállított IP-cím bármely loopback interfészen
3. Ha nincs beállított loopback interfész, akkor a legmagasabb IP-cím bármelyik aktív fizikai interfészen.

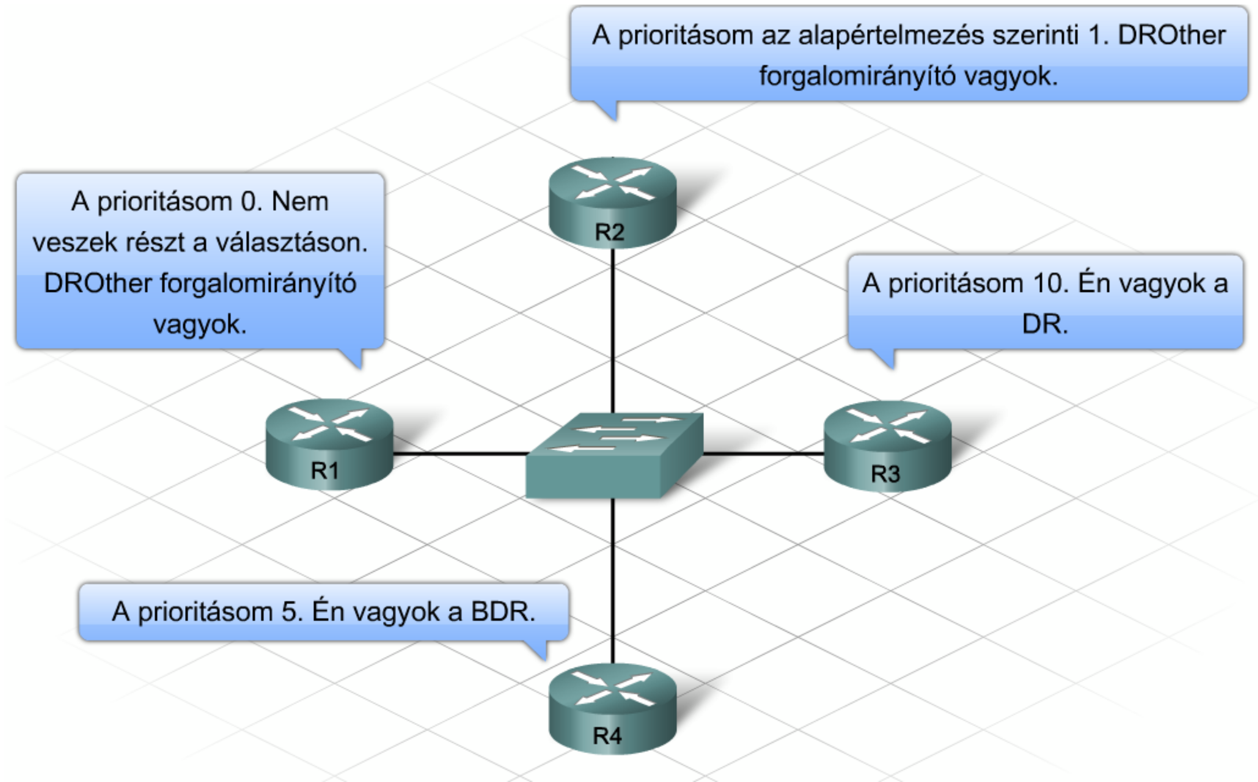
A forgalomirányító azonosítója megtekinthető az alábbi show parancsok alkalmazásával:

`show ip protocols, show ip ospf, show ip ospf interface`

Előfordulhat, hogy a hálózati rendszergazda maga szeretné meghatározni a kijelölt és a tartalék kijelölt forgalomirányítót. Kiválaszthat például egy nagyobb teljesítményű vagy kisebb terheltségű forgalomirányítót erre a célra. Ehhez befolyásolnia kell a DR és BDR választást a megfelelő prioritás beállításával az alábbi parancs segítségével:

`ip ospf priority number`

Alapértelmezett beállítások szerint az OSPF forgalomirányítók prioritása 1. Ha a prioritás értéke megváltozik egy forgalomirányítón, a nagyobb érték nyer a DR és BDR választáson. A legnagyobb beállítható érték a 255. A 0 érték beállításával megakadályozható egy forgalomirányító megválasztása DR-nek vagy BDR-nek.



Nem minden OSPF hálózattípus esetén szükséges kijelölt és tartalék kijelölt forgalomirányító. Az OSPF protokoll az alábbi típusokat különbözteti meg:

Üzenetszórásos többszörös hozzáférésű hálózatok

- Ethernet

Pont-pont (PPP) hálózatok:

- Soros
- T1/E1

Nem szórásos többszörös hozzáférésű (NBMA - Non-Broadcast Multi-Access) hálózatok:

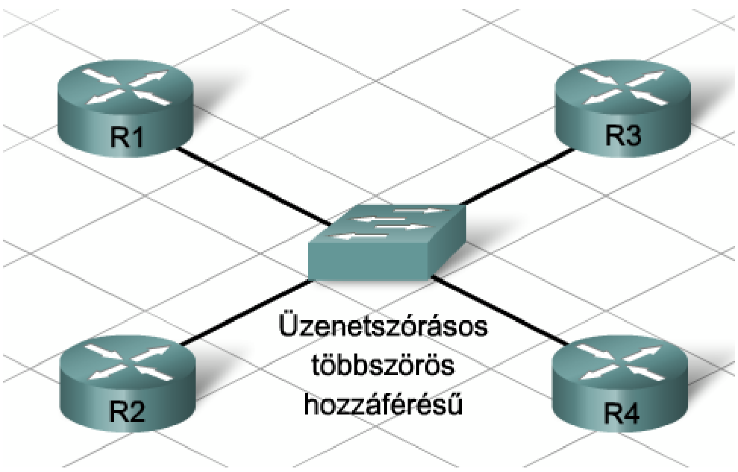
- Frame Relay
- ATM

Üzenetszórásos többszörös hozzáférésű hálózatok esetén, mint az Ethernet is, a szomszédok száma igen sok lehet, ezért szükséges kijelölt forgalomirányító.

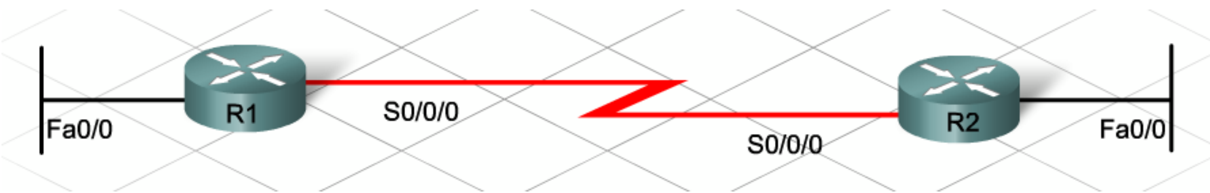
Pont-pont hálózatok esetén teljes értékű szomszédsági viszonyok kialakítása problémamentes, hiszen a hálózattípus természetéből adódóan a kapcsolatban csupán két forgalomirányító vesz részt. Ebben a helyzetben nem szükséges kijelölt forgalomirányítót választani és alkalmazni.

NBMA hálózatok esetén az OSPF protokoll kétféle módban működhet:

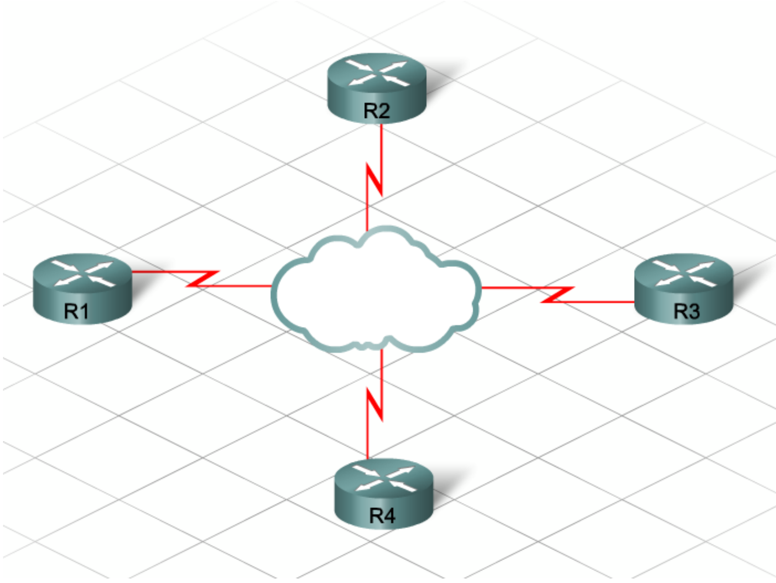
- Szimulált üzenetszórásos környezetben: A rendszergazda beállíthatja a hálózat típusát üzenetszórásosnak, így a hálózat DR és BDR választással üzenetszórásos modellt szimulál. Ilyen esetben általában ajánlott prioritás beállításával meghatározni a kijelölt és a tartalék kijelölt forgalomirányítókat is, és ezzel biztosítani a DR és a BDR kapcsolatát a hálózat összes többi forgalomirányítójával. A szomszédos forgalomirányítók szintén beállíthatók az OSPF konfigurációs módban alkalmazott neighbor parancs segítségével.
- Pont-többpont környezet: Minden, nem üzenetszórásos hálózatot pont-pont kapcsolatok összességeként kezel az OSPF, ezért a DR választás szükségtelen. A szomszédos forgalomirányítókat ebben az esetben is statikusan kell beállítani.



Pont-pont



Nem szórásos többszörös hozzáférésű



6.1.4 OSPF területek

Minden OSPF hálózat kiindulási pontja a 0-s terület, melyet gerinchálózatnak is neveznek. A hálózat növekedésével további területek hozhatók létre a 0-s terület szomszédságában, melyek 65 535-ig bármely számmal jelölhetők. Az egy területhez tartozó forgalomirányítók legnagyobb lehetséges száma 50.

Az OSPF hálózatok kétrétegű, hierarchikus tervezést igényelnek. A 0-s terület, vagy ahogy szintén nevezik, gerinchálózat áll a felső szinten, és az összes többi terület az alsó szinten. Minden területnek, mely nem gerinchálózat, a 0-s területhez közvetlenül kell kapcsolódnia. A területek együttesen alkotnak egy autonóm rendszert (AS - Autonomous System).

Az OSPF adott területen belüli működése különbözik a terület és a gerinchálózat közötti működéstől. A hálózati információk összevonása általában területek között jön létre, aminek segítségével csökkenthető az irányítótáblák mérete a gerinchálózatban. Az összevonás a változások és a bizonytalan összeköttetések hatását a forgalomirányítási tartomány érintett területére korlátozza. Topológia-változás esetén kizárólag az érintett terület forgalomirányítói kapnak LSA hirdetéseket, igy csak ezeknek kell újrafuttatni az SPF algoritmust. A hálózati információk összevonása csak területek között jön létre, aminek segítségével csökkenthető az irányítótáblák mérete a gerinchálózatban. Útvonal-összevonással a topológiaiváltozások és a bizonytalan összeköttetések hatása a forgalomirányítási tartomány érintett területére korlátozható.

A gerinchálózatot más területtel összekötő forgalomirányítót területi határ- forgalomirányítónak (ARB - Area Border Router) nevezik. Egy adott területet a gerinchálózattal összekötő forgalomirányítót területi határ- forgalomirányítónak (ARB - Area Border Router) nevezik. Azokat a forgalomirányítókat, amelyek más irányítóprotokollt, például EIGRP protokollt használó területekhez is kapcsolódnak vagy statikus útvonalakat osztanak meg az OSPF területekkel, autonóm rendszer határ-forgalomirányítónak (ASBR - Autonomous System Border Router) nevezik.

6.2 Egyterületű OSPF megvalósítása

6.2.1 Egyterületű OSPF alapszintű beállítása

Az OSPF protokoll alapszintű beállításához csupán két lépés szükséges. Az elsőben engedélyezni kell az OSPF forgalomirányítást, a másodikban pedig meg kell határozni a hirdetésre kerülő hálózatokat.

1. lépés: Az OSPF engedélyezése

```
router(config)#router ospf <folyamat-azonosító>
```

A folyamatazonosító értékét a rendszergazda választja meg az 1-től 65 535-ig terjedő intervallumból. Csupán helyi jelentőségű (csak az adott forgalomirányítón használt), ezért nem szükséges megegyeznie a többi OSPF forgalomirányítón beállított folyamatazonosítóval.

2. lépés: Hálózatok hirdetése

```
Router(config-router)#network  <hálózati-cím>  <helyettesítő-maszk>  area
<területazonosító>
```

A **network** parancs funkciója megegyezik a más belső irányító protokollok esetén megszokott funkcióval. Egyfelől meghatározza azokat az interfészeket, amelyeken engedélyezett az OSPF csomagok küldése és fogadása, másfelől azonosítja azokat a hálózatokat, amelyeket az OSPF irányítási frissítéseinek tartalmaznia kell.

Az OSPF **network** parancs egy hálózati cím és egy helyettesítő maszk (wildcard mask) együttesét használja, ezek közösen jelölik ki az OSPF OSPF számára engedélyezett interfészeket, és hálózatokat.

A területazonosító (area ID) meghatározza azt a területet, melyhez a hálózat tartozik. Ha nincsenek területek definiálva, a 0-s területet akkor is fel kell tüntetni. Egyterületű OSPF környezetben a területazonosító mindig 0.

Az OSPF network parancs alkalmazásánál a helyettesítő maszkot minden esetben meg kell adni. Útvonalösszegzés és szuperhálózatok használata esetén a helyettesítő maszk az alhálózati maszk inverze.

Egy hálózat vagy alhálózat helyettesítő maszkjának meghatározásához az interfész decimális alhálózati maszkját egyszerűen ki kell vonni a csupa 255-ös maszkból (255.255.255.255).

Például egy rendszergazda a 10.10.10.0/24-es alhálózatot szeretné hirdetni az OSPF protokoll esetén. Mivel ebben az esetben az alhálózati maszk /24, azaz 255.255.255.0, a helyettesítő maszk kiszámításához ezt kell kivonni a csupa 255-ös maszkból.

Csupa 255-ös maszk: 255.255.255.255
Alhálózati maszk: - 255.255.255.0

Helyettesítő maszk: 0. 0 . 0 .255

A számítás alapján az OSPF network parancs formája:

```
Router(config-router)#network 10.10.10.0 0.0.0.255 area 0
```

Network parancs:
`R2(config-router)#network 172.16.4.0 0.0.0.255 area 0`

1. példa:	
Hálózat	172.16.4.0 /24
Csupa 255-ös maszk	255.255.255.255
Alhálózati maszk	- 255.255.255.0
Helyettesítő maszk	0.0.0.255

Network parancs:
`R1(config-router)#network 172.16.1.16 0.0.0.15 area 0`

2. példa:	
Hálózat	172.16.1.16 /28
Csupa 255-ös maszk	255.255.255.255
Alhálózati maszk	- 255.255.255.240
Helyettesítő maszk	0.0.0.15

Network parancs:
`R3(config-router)#network 192.168.10.4 0.0.0.3 area 0`

3. példa:	
Hálózat	192.168.10.4 /30
Csupa 255-ös maszk	255.255.255.255
Alhálózati maszk	- 255.255.255.252
Helyettesítő maszk	0.0.0.3

További információ

A network parancs alkalmazásánál az alhálózattal egybeeső címtartomány megadása helyett, használhatja az interfész (állomás) IP-címét és a 0.0.0.0 maszkot. Ez korlátozza az OSPF hirdetéseket erre a meghatározott interfészre és címre, mivel mind a 32 címbitnek egyeznie kell. Példa: `Router(config-router)#network 10.10.10.1 0.0.0.0 area 0`

6.2.2 Az OSPF hitelesítés beállítása

Az OSPF, más irányítóprotokollokhoz hasonlóan, a szomszédok közötti információcserét alapértelmezetten nyílt szövegként bonyolítja le, és ezzel a hálózat ellen irányuló biztonsági fenyegetésre ad lehetőséget. Csomagelemző alkalmazás segítségével ugyanis egy hacker elfoghatja és elolvashatja az OSPF frissítéseket, melyekből hálózati információkat nyerhet.

E biztonsági probléma elhárítható a forgalomirányítók közötti OSPF hitelesítés konfigurálásával. Ha egy területen a hitelesítés engedélyezett, a forgalomirányítók csak akkor osztják meg egymással az információkat, ha a hitelesítési adatok megegyeznek.

Egyszerű jelszavas hitelesítés esetén, minden forgalomirányítón egy kulcsnak nevezett jelszót kell beállítani. A módszer csupán alapszintű védelmet nyújt, mert a forgalomirányítók nyílt szövegben küldik a jelszót, így az elolvasásuk csak annyira nehéz, amennyire a nyílt szöveg elolvasása.

Biztonságosabb hitelesítési eljárást jelent a Message Digest 5 (MD5) titkosítás. Ez egy kulcs és egy kulcsazonosító beállítását igényli az összes forgalomirányítón. A forgalomirányító a kulcsból, az OSPF csomagból és a kulcsazonosítóból egy algoritmus alkalmazásával létrehoz egy titkosított számot,

amely belekerül minden OSPF csomagba. A csomagellenőrző alkalmazások használatával a kulcs nem szerezhető meg, hiszen nem kerül továbbításra a hálózaton.

```
R1(config)#router ospf 18
R1(config-router)#network 10.0.0.0  0.0.0.255 area 0
R1(config-router)#area 0 authentication message-digest
R1(config)#interface serial0/0/0
R1(config-if)#ip address 10.0.0.1 255.255.255.0
R1(config-if)#ip ospf message-digest-key 10 md5 areapassword
```

6.2.3 Az OSPF paraméterek beállítása

Az OSPF protokoll alapszintű beállításánál a rendszergazdának gyakran szüksége van bizonyos OSPF paraméterek megváltoztatására.

Ilyen eset lehet például, amikor a rendszergazda szeretné meghatározni, hogy melyik forgalomirányító legyen a DR és melyik a BDR. Az interfész prioritásának vagy a forgalomirányító azonosítójának beállításával ez a feladat teljesíthető.

A kijelölt forgalomirányító megválasztása az alábbi sorrend szerint, a felsorolt paraméterek legmagasabb értéke alapján történik:

1. **Interfész prioritás:** Az interfész prioritása a `priority` parancs alkalmazásával állítható be.
2. **Forgalomirányító azonosító:** A forgalomirányító azonosító a `router-id` parancs alkalmazásával állítható be.
3. **Legmagasabb loopback-cím:** Alapértelmezésben a forgalomirányító azonosítója a legmagasabb IP-címmel rendelkező loopback interfész IP-címe. Az OSPF előnyben részesíti a loopback interfészeket, mivel azok logikai és nem fizikai interfészek. A logikai interfészek mindig működnek.
4. **A fizikai interfészek legmagasabb címe:** A forgalomirányító az aktív interfészeinek címei közül a legmagasabb IP-címet használja a forgalomirányító azonosítójaként. Ez a lehetőség problémát okozhat, ha az interfész meghibásodik vagy újrakonfigurálják.

Miután megváltozik egy forgalomirányító azonosítója vagy prioritása, a szomszédsági viszonyokat alaphelyzetbe kell állítani.

A `clear ip ospf process` parancs alkalmazásával biztosítható az új értékek érvénybelépése. Ez a parancs biztosítja az új érték érvénybe lépését.

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip ospf priority 50
```

```
R1(config)#router ospf 1
R1(config-router)#router-id 10.1.1.1
```

```
R1(config)#interface loopback 1
R1(config-if)#ip address 10.1.1.1 255.255.255.255
```

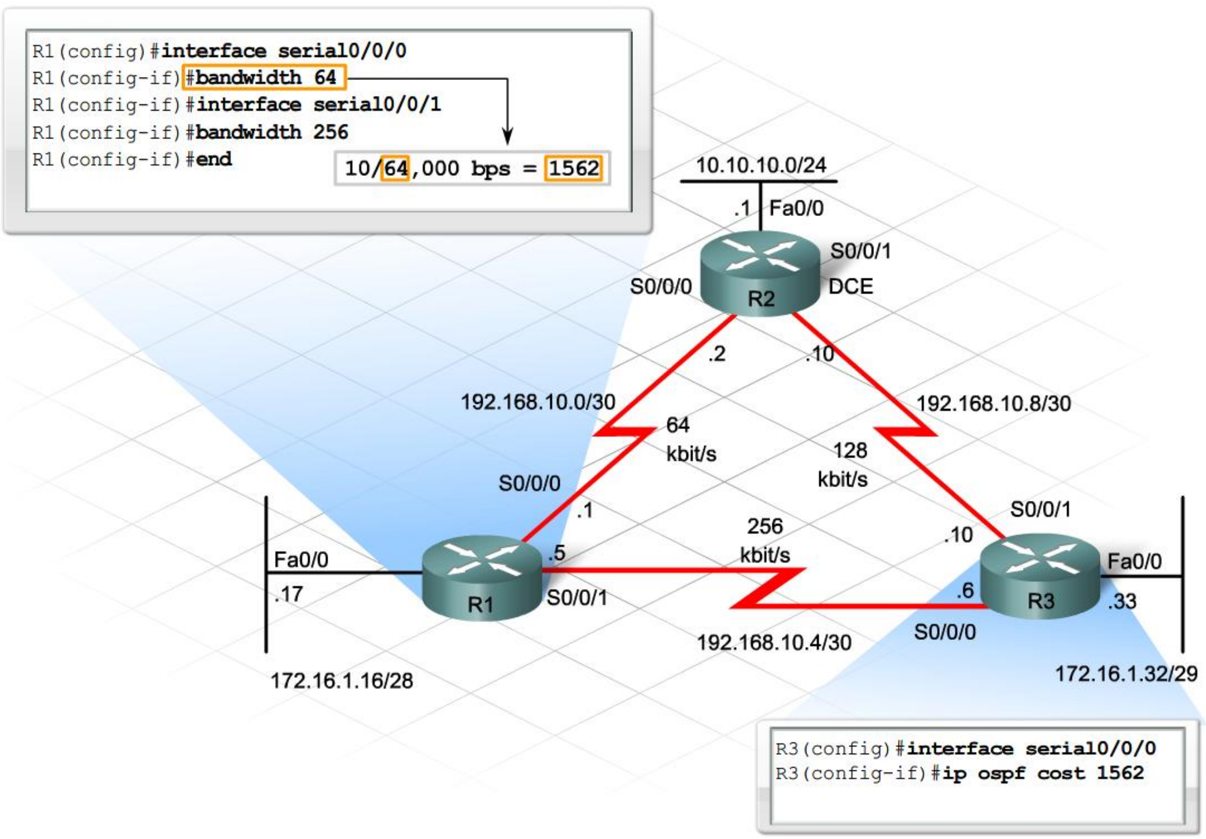
A sávszélesség is olyan paraméter, amely gyakori módosítást igényelhet. A Cisco forgalomirányítókon a legtöbb soros interfész sávszélességének alapértelmezett beállítása 1.544 Mbit/s, azaz a T1 kapcsolat sebessége. Ez az érték meghatározza a kapcsolat OSPF költségét, de valójában nem függ össze a kapcsolat sebességével.

Bizonyos körülmények között egy szervezet részleges T1 kapcsolatot kap az internetszolgáltatótól. Részleges T1 kapcsolat például a T1 kapcsolat egynegyed része, azaz 384 Kbit/s. Az IOS a T1 kapcsolat alapértelmezett teljes sávszélességét érzékeli a soros kapcsolaton, még ha az csak 384 Kbit/s is. A hibás érzékelés helytelen útválasztást eredményez, mivel a kapcsolatot az irányító protokollok a ténylegesnél gyorsabb kapcsolatként veszik számításba.

Amikor a soros interfész nem az alapértelmezett T1 sebességgel működik, a megfelelő bandwidth érték kézi beállítása szükséges. A kapcsolat mindkét végpontján ugyanazt az értéket kell konfigurálni.

OSPF esetén a `bandwidth interface` és az `ip ospf cost interface` parancsok alkalmazásával végrehajtott módosítások azonos eredményre vezetnek. Mindkét parancs pontos értéket határoz meg az OSPF protokoll számára a legjobb útvonal meghatározásához.

A `bandwidth` parancs megváltoztatja az OSPF költségmértékének meghatározásához használt sávszélesség értékét. A költség közvetlen megváltoztatására az ip ospf cost parancs használható.



Az OSPF protokoll költségmértékéhez kapcsolódó további paraméter a referencia-sávszélesség, amely az interfész költségének, más néven a kapcsolat költségének (link cost) kiszámításához szükséges.

Az egyes interfészek esetén a sávszélesség-értékének meghatározása a következő képlettel történik: 100 000 000/sávszélesség. A 100 000 000 (10^8) érték az ún. referencia-sávszélesség érték.

Problémát okoznak a nagyobb sebességű összeköttetések, például a Gigabit Ethernet és a 10Gbit Ethernet. Az alapértelmezett 100 000 000 referencia-sávszélességű vagy az ennél gyorsabb kapcsolatok OSPF költsége egységesen 1.

Pontosabb költségszámítások érdekében szükséges lehet a referencia-sávszélesség értékének módosítása, mely az `auto-cost reference-bandwidth` paranccsal hajtható végre.

Amennyiben szükség van ennek a parancsnak a használatára, akkor az OSPF mérték következetességének érdekében minden forgalomirányítón egységesen kell alkalmazni a beállítást. Az új referencia-sávszélesség Mbit/s –ban adható meg. Például, 10-Gigabit referencia-sávszélesség megadása esetén a megfelelő érték 10 000.

6.2.4 Az OSPF működésének ellenőrzése

Az OSPF esetén számos parancs áll rendelkezésre a megfelelő működés ellenőrzéséhez.

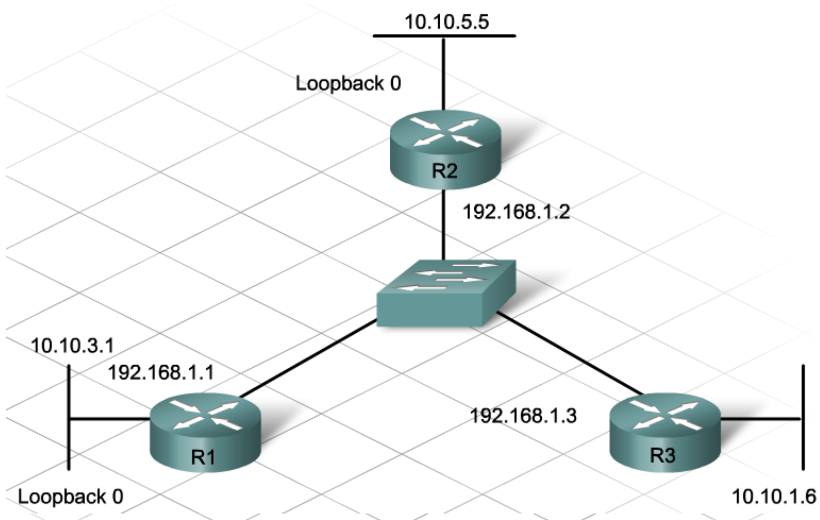
Az OSPF hálózat hibaelhárításánál jól alkalmazható a `show ip ospf neighbor` parancs, mellyel a szomszédsági viszonyok kialakítása ellenőrizhető.

Ha a szomszéd forgalomirányító azonosítója nem jelenik meg, vagy nincs teljes értékű állapotban, a két forgalomirányító között nem alakult ki szomszédsági viszony. DROther forgalomirányító esetén szomszédsági viszony teljes értékű vagy két utas állapot esetén jön létre.

Többszörös hozzáférésű Ethernet hálózat esetén a DR és BDR szerep csak a teljes értékű szomszédsági állapot beálltát követően válik láthatóvá az állapot oszlopban.

Két forgalomirányító között nem jön létre szomszédsági viszony, ha:

- az alhálózati maszkok különbözősége miatt a forgalomirányítók nem azonos hálózathoz tartoznak
- az OSPF hello és várakozási időzítői nem egyeznek meg
- az OSPF hálózat típusa nem egyezik
- hiányos vagy helytelen valamelyik network parancs



R1#show ip ospf neighbor

Szomszédazonosító	Prioritás	Állapot	"Halott" időzítő	Cím	Interfész
10.10.5.5	1	FULL/DR	00:00:37	192.168.1.2	FastEthernet 0/0
10.10.1.6	1	2WAY/DROther	00:00:15	192.168.1.3	FastEthernet 0/0

Szomszédazonosító: A szomszéd forgalomirányító-azonosítója.
Prioritás: A forgalomirányító interfészének prioritása.
Állapot: A szomszédsági kapcsolat állapota.
"Halott " időzítő: Az az idő, amíg a forgalomirányító várakozik anélkül, hogy a szomszéd forgalomirányítótól hello csomagot kapna és halottnak nyilvánítaná.
Cím: A szomszéd interfészének IP-címe.
Interfész: Ennek a forgalomirányítónak az az interfésze, amelyikkel a szomszédsági viszonyt kialakítja a szomszéd forgalomirányító felé.

Több show parancs is alkalmas az OSPF működésének ellenőrzésére.

```
show ip protocols
```

Megjeleníti a forgalomirányító azonosítóját, a meghirdetett hálózatokat és a szomszédsági viszonyban lévő forgalomirányítók IP-címét.

```
show ip ospf
```

Megjeleníti a forgalomirányító azonosítóját és az OSPF folyamatának, időzítőinek és területi információjának részleteit.

```
show ip ospf interface
```

Megjeleníti a forgalomirányító azonosítóját, a hálózat típusának költségét és az időzítők beállításait.

```
show ip route
```

Információt ad arra vonatkozóan, hogy a forgalomirányító kap-e és küld-e OSPF útvonal információt.

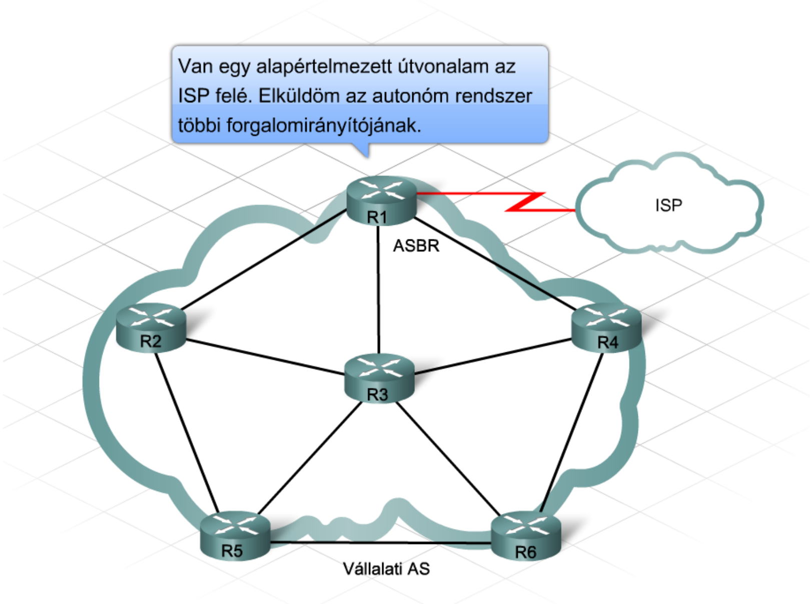
6.3 Több irányítóprotokoll együttes alkalmazása

6.3.1 Alapértelmezett útvonal beállítása és meghirdetése

A legtöbb hálózat interneten keresztül kapcsolódik egymáshoz. Az OSPF protokoll egy autonóm rendszeren belül biztosít forgalomirányítási információkat. Továbbá adatokkal szolgál az autonóm rendszeren kívüli, elérhető hálózatokról is.

Bizonyos esetekben némely forgalomirányítón a rendszergazda statikus útvonalakat állít be, amelyeket az irányító protokollok alapértelmezetten nem terjesztenek. Nagy hálózat esetén igen körülményes feladat a statikus útvonalak konfigurálása az összes forgalomirányítón. Ennél egyszerűbb eljárás az internet felé vezető alapértelmezett útvonal beállítása.

OSPF esetén a rendszergazda ezt az útvonalat rendszerint egy ún. ASBR forgalomirányítón (Autonomous System Boundary Router / Autonomous System Border Router) konfigurálja. Az ASBR forgalomirányító kapcsolatot teremt az OSPF hálózat és a külvilág között. Miután az irányítótáblájába bekerült a megfelelő alapértelmezett útvonal beállítható, hogy az ABSR forgalomirányító a többi forgalomirányító felé hirdesse azt. Amint egy alapértelmezett útvonal bekerül az irányítótáblájába, megfelelő beállítással a forgalomirányító hirdetni fogja az OSPF hálózat többi része felé. Ez a hirdetett útvonal kijáratként szolgál az OSPF hálózat többi része számára. Az eljárás lehetővé teszi az AS minden forgalomirányítójának tájékoztatását az alapértelmezett útvonalról, és megkíméli a rendszergazdát alapértelmezett útvonalak statikus konfigurálásától az egyes forgalomirányítókon.



Az alapértelmezett útvonal az OSPF hálózaton belüli terjesztéséhez az alábbi lépések szükségesek:

1. lépés

Alapértelmezett útvonal konfigurálása az ASBR forgalomirányítón.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0
```

Az ip route parancs alkalmazása során vagy egy interfészt vagy a következő ugrás IP-címét kell megadni.

2. lépés

ASBR forgalomirányító konfigurálása az alapértelmezett útvonal hirdetésére. Alapértelmezés szerint, az OSPF protokoll hirdetései még akkor sem tartalmazzák az alapértelmezett útvonalat, ha az már szerepel az irányítótáblában.

```
R1(config)#router ospf 1
R1(config-router)#default-information originate
```

A fenti parancsok eredményeként az OSPF tartomány forgalomirányítóinak irányítótáblájában megjelenik egy végső (last resort) átjáró és a 0.0.0.0/0 hálózat. Az így bejegyzett alapértelmezett útvonal az irányítótáblában külső útvonalként (E2) látszik.

6.3.2 Az OSPF útvonalösszegzés beállítása

Az OSPF útvonalösszegzés megkönnyítése érdekében az IP-címeket a területeknek megfelelően érdemes csoportosítani. Az alábbi példában egy OSPF területhez a következő négy, folytonos hálózati szegmens tartozik:

- 192.168.0.0/24
- 192.168.1.0/24
- 192.168.2.0/24
- 192.168.3.0/24

Ez a négy hálózat összevonható és egyetlen hálózatként hirdethető a 192.168.0.0/22 címmel. Az útvonalösszevonás az OSPF tartományban csökkenti a meghirdetett hálózatok számát, a szükséges memória nagyságát és a forgalomirányító frissítéseiben szereplő bejegyzések számát.

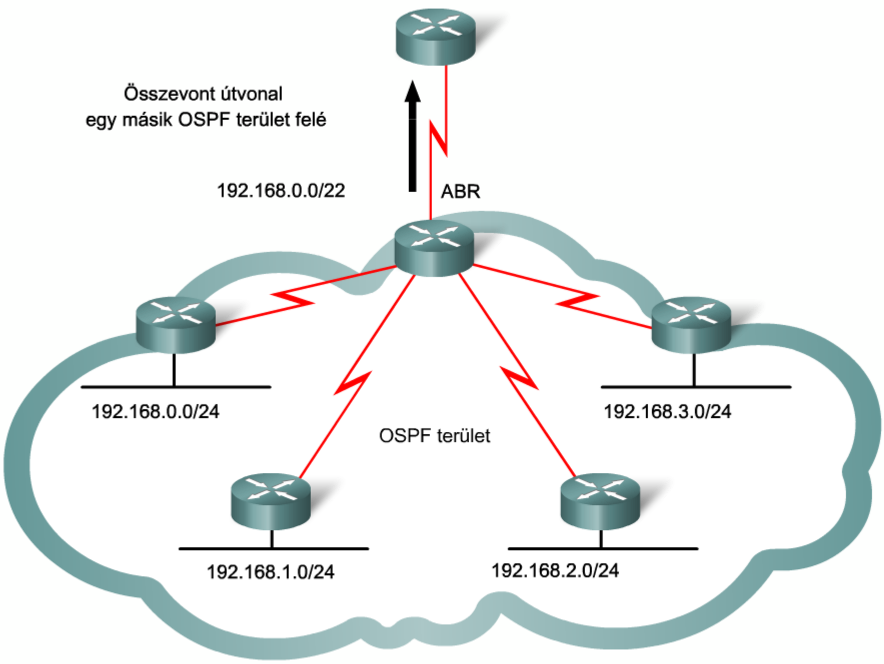
Továbbá előnyt jelent, hogy az összevonás mérsékli a folyamatosan eltűnő, majd újramegjelenő ún. váltakozó útvonalak (flapping route) negatív hatását. A vergődés olyan útvonalra utal, amely folyamatosan változik a működő és a működésképtelen állapot között. Alapértelmezésben egy váltakozó (hol működő, hol lekapcsolt állapotú) útvonal minden állapotváltozása útvonalfrissítést eredményez az egész tartományban, s ez jelentősen megnöveli a hálózat forgalmát és terheltségét.

Amikor egy forgalomirányító útvonalösszevonást alkalmaz, egyetlen, szuperhálózat-címmel jelöl több útvonalat. Az útvonalak közül elég csupán egy működőképessége ahhoz, hogy a forgalomirányító meghirdethesse az összevont útvonalat. Abban az esetben ha az útvonalak között van egy vagy több váltakozó útvonal, a forgalomirányító továbbra is csak a sokkal stabilabb összevont útvonalat fogja hirdetni, és az egyes különálló útvonalakról egyáltalán nem továbbít frissítést. Az útvonalösszevonást végző forgalomirányító bármely váltakozó útvonalon továbbítandó csomagot egyszerűen eldobja, amíg az adott útvonal működésképtelen.

Az OSPF ASBR eszköz forgalomirányító konfigurációs üzemmódjában az alábbi parancs segítségével konfigurálható összevont útvonal:

```
area terület-azonosító range IP-cím maszk
```

A parancson belül meg kell határozni azt a területet, amelyen az útvonalösszegzés történik, valamint a kezdő hálózat címét és alhálózati maszkját.



6.3.3 Az OSPF problémái és korlátai

Az OSPF egy bővíthető irányító protokoll. Gyors konvergenciára képes és nagy hálózatokban is alkalmazható. Ennek ellenére a használata során néhány problémával kell szembenézni.

Az OSPF több adatbázist is karbantart, ezért nagyobb memória- és CPU kapacitásra van szüksége, mint a távolságvektor alapú irányító protokolloknak.

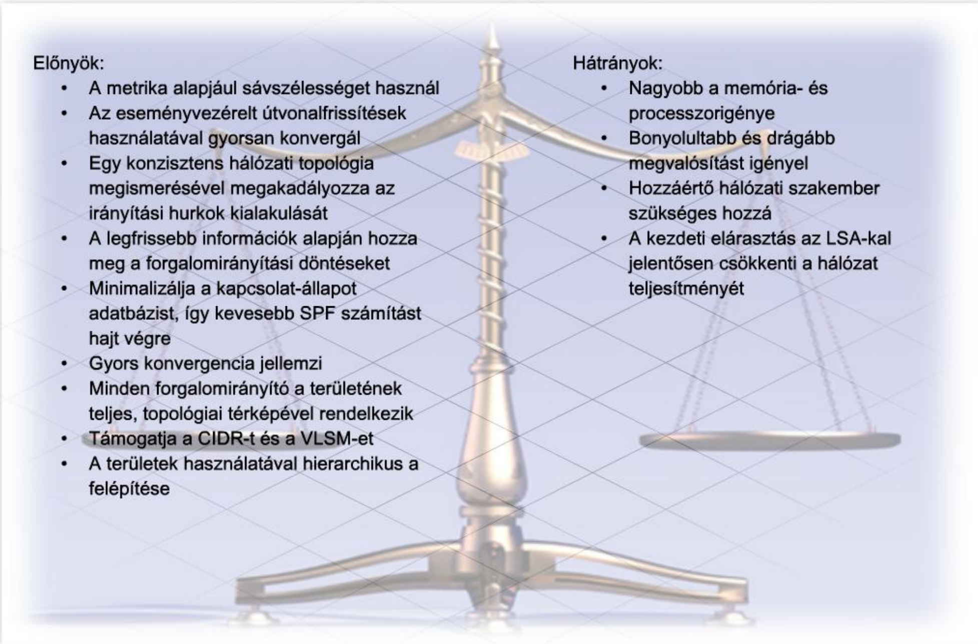
A Dijkstra algoritmus a legjobb útvonal meghatározásához a CPU-t nagymértékben igénybe veszi. Ha az OSPF hálózat bonyolult és nem stabil, a gyakori újraszámolás következtében az algoritmus erőforrás használata jelentős lehet. Az OSPF protokollt futtató forgalomirányítók általában nagyobb teljesítményűek és ezért drágábbak.

A túlzott erőforrás-használat elkerülése érdekében, a hálózatot ajánlott kisebb területekre osztani egy szigorú, hierarchikus tervezés alkalmazásával. Minden területnek a 0-s területhez kell kapcsolódnia, különben elveszíthetik a kapcsolatot a többi területtel.

Az OSPF protokoll lehetővé teszi nagy és bonyolult hálózatok tervezését, azonban az OSPF adatbázisokban és irányítótáblában tárolt adatok értelmezése a technológia magas szintű ismeretét követeli meg.

A kezdeti, feltérképező folyamat során, az OSPF LSA hirdetések elárasztják a hálózatot, korlátozva ezzel a felhasználói adatok továbbítását. Kis sávszélességgel rendelkező, sok forgalomirányítót tartalmazó kiterjedt hálózatokban az elárasztás jelentősen csökkentheti a hálózat teljesítményét.

Korlátai és problémái ellenére vállalati hálózatokban az OSPF protokoll a legszélesebb körben alkalmazott irányító protokoll.

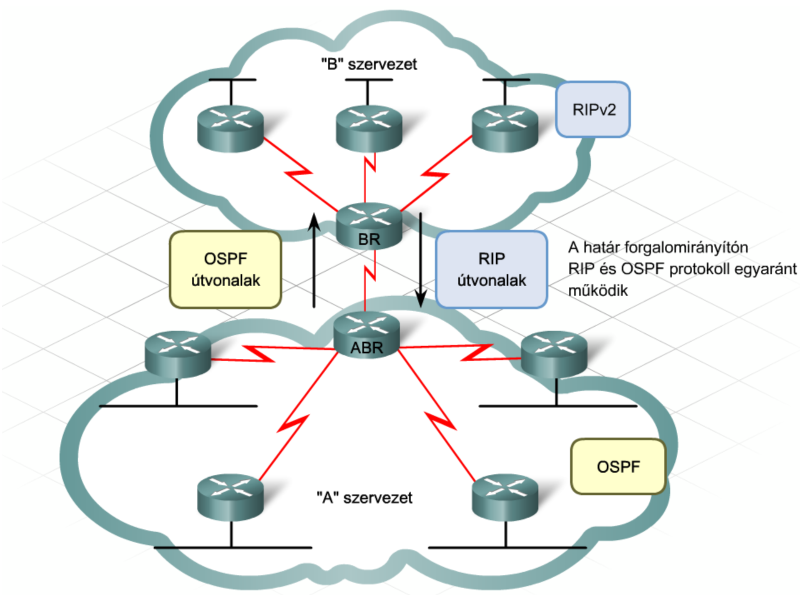


6.3.4 Több protokoll egyidejű alkalmazása nagyvállalati környezetben

Egyes szervezetek többfajta irányító protokollt is használnak, aminek számos oka lehet.

- A hálózati rendszergazda a hálózat különböző részein különböző protokollokat alkalmazhat a rendelkezésre álló, hagyományos eszközökhöz vagy az elérhető erőforrásokhoz igazodva.
- Elképzelhető, hogy két cég, ami különböző irányítóprotokollt használ, egyesül, és szükség van az egymás közötti kommunikációra.

Amikor több irányító protokoll fut egyetlen forgalomirányítón, előfordulhat, hogy ugyanazt az útvonalat a forgalomirányító több forrásból is megtanulja. Ilyen esetben elengedhetetlen egy olyan jól meghatározott módszer a forgalomirányító számára, amellyel kiválaszthatja a legmegfelelőbb útvonalat és elhelyezheti az irányítótáblában.



Az "A" és a "B" szervezet egyesül

Amikor egy forgalomirányító egyetlen hálózatról több forrásból is értesül, az adminisztratív távolság (AD - administrative distance) figyelembevételével határozza meg az előnyben részesített útvonalat. A Cisco IOS minden irányítási információt alkalmazó módszerhez egy adminisztratív távolságot rendel.

Ha egy forgalomirányító egy meghatározott alhálózatról RIP és OSPF forrásból is értesül, az OSPF által tanult útvonalat fogja előnybe részesiteni és eltárolni az irányítótáblában. Az irányítótábla bejegyzéseinek elején látható kód jelzi az útvonal forrását, vagy a tanulás módját. Minden kódhoz meghatározott AD tartozik.

Az útvonal forrása	Adminisztratív távolság	Alapértelmezett mérték(ek)
Csatlakoztatva	0	0
Statikus	1	0
EIGRP összevont útvonal	5	0
Külső BGP	20	Sávszélesség, késleltetés
Belső EIGRP	90	A kapcsolat költsége (sávszélesség)
IGRP	100	A kapcsolat költsége (sávszélesség)
OSPF	110	Ugrásszám
IS-IS	115	Rendszergazda által megadott érték
RIP	120	
Külső EIGRP	170	
Belső BGP	200	

Ha két hálózat azonos hálózati címmel és alhálózati maszkkal rendelkezik, akkor a forgalomirányítók azonosnak látják őket. Ez a megállapítás akkor is igaz, ha a két hálózat közül az egyik egy összevont hálózat, a másik pedig az összevonásban szereplő valamelyik önálló hálózat.

Annak ellenére, hogy a 192.168.0.0/22 összevont hálózat tartalmazza a 192.168.1.0/24 hálózatot, külön bejegyzésként szerepelnek. Ilyen esetekben mindkét bejegyzés megtalálható az irányítótáblában. Annak eldöntésére, hogy melyik útvonal legyen használatban, a leghosszabb előtag-egyezés szolgál.

Például, egy forgalomirányító csomagot kap a 172.16.0.10 célcímmel. Három lehetséges útvonalnak felel meg: 172.16.0.0/12, 172.16.0.0/18, és. Közülük a 172.16.0.0/26 mutatja a leghosszabb egyezést. Egyezésről akkor beszélhetünk, ha legalább az alhálózati maszkban jelzett bitszámig megegyezik binárisan a célcím és az adott útvonal.

1. példa	Cél IP-címe	
Cél	192.168.1.15	11000000.10101000.00000001.00001111
1. útvonal	O 192.168.0.0/22[110/65]via 192.168.0.1 serial 0/0/0	11000000.10101000.00000000.00000000
2. útvonal	O 192.168.1.0/24[110/65]via 192.168.1.1 serial 0/0/1	11000000.10101000.00000001.00000000

Leghosszabb egyezés a cél IP-címmel

1. példa	Cél IP-címe	
Cél	192.168.3.23	11000000.10101000.00000011.00010111
1. útvonal	O 192.168.0.0/22[110/65]via 192.168.0.1 serial 0/0/0	11000000.10101000.00000000.00000000
2. útvonal	O 192.168.1.0/24[110/65]via 192.168.1.1 serial 0/0/1	11000000.10101000.00000001.00000000

Leghosszabb egyezés a cél IP-címmel

6.4 A fejezet összefoglalása

- Skálázhatóságot, útvonal-összevonást és a problémák elszigetelhetőségét teszi lehetővé.
- A költség-mértéket a sávszélesség alapján számolja ki.
- Egy terület forgalomirányítói a szomszédjaik kapcsolatainak állapotáról adnak hírt LSA-k segítségével.
- Többszörös hozzáférésű hálózatban az OSPF forgalomirányítók kijelölt és tartalék kijelölt forgalomirányítót választanak.
- OSPF autonóm rendszer megtervezése a gerinchálózattal, más néven a 0-ás területtel kezdődik. Minden más terület a 0-ás terület szomszédja.
- Az ABR forgalomirányító a 0-ás területet köti össze más területekkel.
- Az ASBR forgalomirányító a teljes OSPF autonóm rendszert köti össze más autonóm rendszerekkel.
- Az OSPF network parancs a hálózati cím és a helyettesítő maszk kombinációját használja, mely egy interfész-címet vagy egy címtartományt engedélyez az OSPF számára.
- Az OSPF útvonalfrissítések biztonsága érdekében a forgalomirányítók között hitelesítés állítható be. A legbiztonságosabb hitelesítő eljárás az MD5.
- A hálózati rendszergazda prioritás vagy azonosító beállításával irányíthatja a DR és BDR választás kimenetelét.
- A bandwidth interface és az ip ospf cost interface parancs biztosítja, hogy az OSPF a legjobb útvonal kiválasztásánál a jelenleg érvényben levő költséget használja.
- Számos show parancs alkalmazható az OSPF működésének ellenőrzésére, mint például a show ip protocols, show ip ospf, show ip ospf interface, show ip route és show ip ospf neighbor.
- Egy rendszergazda alapértelmezett útvonalat konfigurál egy ASBR forgalomirányítón, majd beállítja a meghirdetését az OSPF hálózat többi része felé.
- Területek közötti útvonal-összevonást a területi határ-forgalomirányítókon (ABR) kell konfigurálni és az autonóm rendszeren belül segíti a forgalomirányítást. Az autonóm rendszerek közötti útvonal-összevonást az Autonóm rendszer Határ-forgalomirányítón (ASBR) kell beállítani.
- Az OSPF több memória és CPU erőforrást igényel, így nagyobb teljesítményű és költségesebb forgalomirányítókra van szükség.
- Az útvonalelosztás lehetővé teszi egy irányító protokoll vagy statikus útvonal beillesztését egy másik irányító protokollba.
- Az adminisztratív távolság és a leghosszabb egyező prefix meghatározza a legjobb útvonalat egy hálózat felé.

7. Vállalati WAN kapcsolatok megvalósítása

7.1 A vállalati WAN hálózatok összekapcsolása

7.1.1 WAN eszközök és technológiák

Ahogy a vállalatok növekednek, gyakori, hogy az egytelephelyes cégből többtelephelyes lesz. Ez a bővülés általában kikényszeríti a vállalati hálózat bővülését, igy a helyi hálózati (Local Area Network, LAN) szint mellett a nagykiterjedésű hálózatok (Wide Area Network, WAN) megjelenését is.

Egy helyi hálózat rendszergazdája még fizikailag is képes a teljes hálózati kábelezés, az eszközök és a szolgáltatások felügyeletére. Annak ellenére, hogy néhány nagyobb vállalat saját WAN hálózat üzemeltet, a legtöbb szervezet valamilyen szolgáltatótól vásárolja a WAN szolgáltatásokat. A szolgáltatók használati díjat számolnak fel hálózati erőforrásaik igénybevételéért. Az internetszolgáltatók (Internet Service Provider, ISP) segítségével a felhasználók megoszthatják az erőforrásaikat a távoli helyeik között, anélkül, hogy számolniuk kellene egy saját hálózat megépítésének és fenntartásának költségeivel.

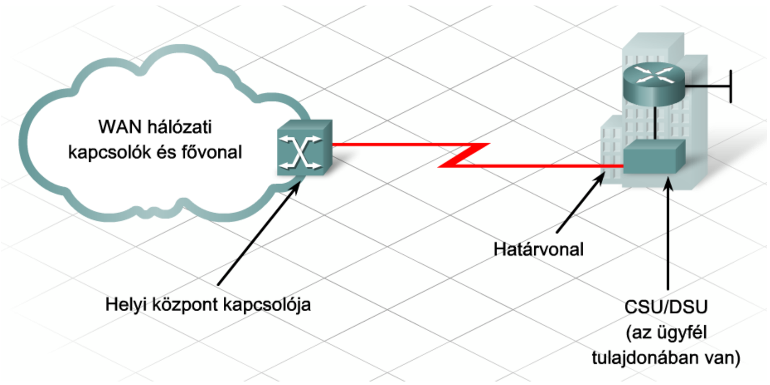
A LAN-ok és WAN-ok között nemcsak a hálózati erőforrások felügyeletében van különbség. A technológiák is eltérőek. A leggyakoribb LAN technológia az Ethernet. A WAN technológiák viszont soros átvitelt valósítanak meg. A soros átvitel lehetővé teszi a megbízható, nagytávolságú kommunikációt, de a helyi hálózatoknál alacsonyabb sebességeken.

WAN-kapcsolatok megvalósításakor az alkalmazott WAN technológia szabja meg az ehhez szükséges eszközök típusát. A WAN hálózatokhoz való kapcsolódáskor például átjáróként forgalomirányítót használunk, amely a szolgáltató hálózata számára kezelhető formátumúvá alakítja az adatokat. A modemek és az ezekhez hasonló, átalakító szerepet betöltő eszközök (translation device), az adatok szolgáltatói hálózaton keresztül történő átvitelét készítik elő.

Digitális vonalak esetén csatornaszolgáltató (Channel Service Unit, CSU) és adatszolgáltató (Data Service Unit, DSU) egységekre van szükség az adatok előkészítésére a WAN-kapcsolaton történő adat-továbbításhoz. Ez a két eszköz gyakran egyetlen berendezésben egyesítve fordul elő, melyet CSU/DSU-nak nevezünk. Ez az eszköz többnyire a forgalomirányítók interfészkártyájába van beépítve. Analóg kapcsolatok esetén modemre van szükség.

Amikor egy vállalat valamilyen WAN szolgáltatásra fizet elő akkor a szolgáltató birtokolja és tartja fent a szükséges berendezéseket. Bizonyos esetekben azonban az előfizető tulajdonában is van néhány kommunikációs eszköz, melyek működéséért maga felel. Azon a ponton, ahol az ügyfél felügyeleti feladatai és felelősségi kötelezettségei véget érnek, ott kezdődik a szolgáltató felügyeleti és felelősségi feladatköre. . Ezt a pontot demarkációs pontnak nevezzük (demarcation point, demarc). A demarkációs pont elhelyezkedhet például a forgalomirányító és az átalakító berendezés között de akár az átalakító berendezés és a szolgáltató központi irodája (Central Office, CO) közötti vonal csatlakozásánál. Tekintet nélkül a tulajdonjogra, a szolgáltatók az előfizetői végberendezés

(Customer Premise Equipment, CPE) kifejezést használják az ügyfél telephelyén elhelyezkedő berendezés megjelölésére.

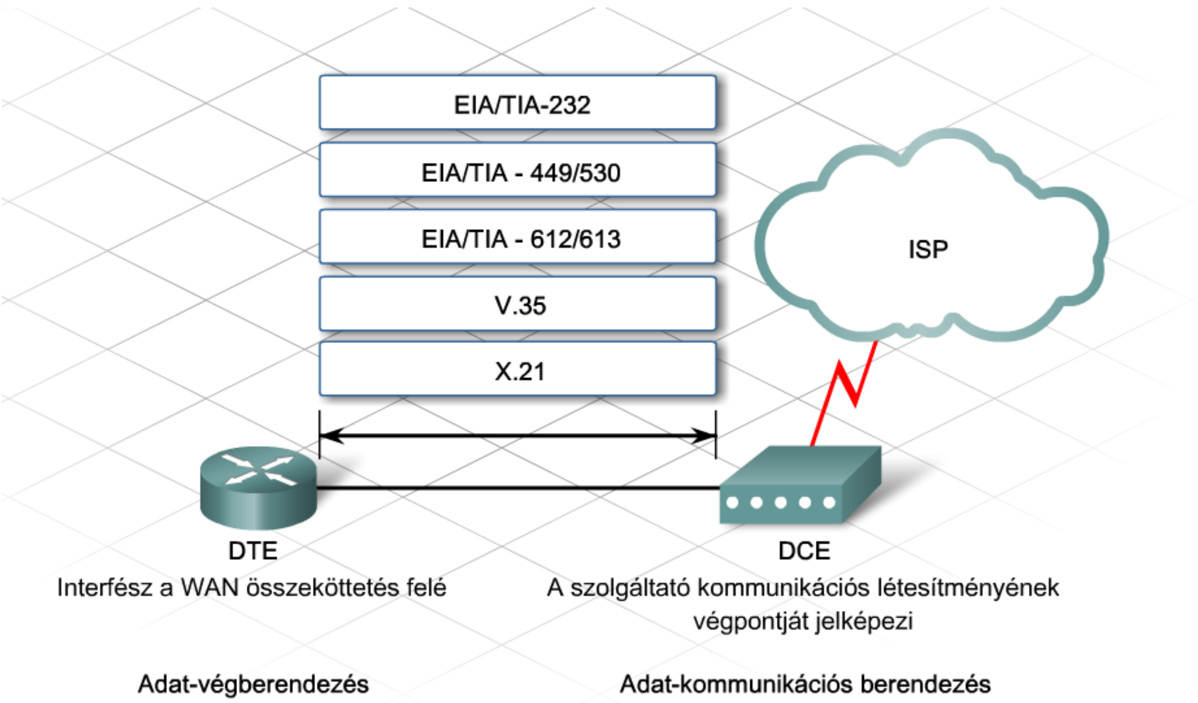


A központi iroda (CO) az a hely, ahol a szolgáltató a berendezéseit tárolja, és fogadja az ügyfélkapcsolatokat. A CPE-től kiinduló fizikai vonal réz vagy optikai kábelt használva csatlakozik a központi irodában elhelyezett forgalomirányítóhoz vagy WAN kapcsolóhoz.

Ez a kapcsolat az úgynevezett helyi hurok vagy „utolsó mérföld” (last mile). Az ügyfél szemszögéből ez a „első mérföld” (first mile), mivel ez az ügyfél telephelyéről kivezető átviteli közeg első szakasza.

A CSU/DSU vagy a modem feladata a helyi hurok felé tartó adatok mozgásának ütemezése, valamint az órajel biztosítása a forgalomirányító számára. A CSU/DSU adatkommunikációs (Data Communications Equipment, DCE) eszköznek minősül. A DCE felé tartó adatok továbbításáért felelős forgalomirányító viszont az adat-végberendezések (Data Terminal Equipment, DTE) csoportjába tartozik.

A DTE/DCE interfész számos fizikai rétegbeli protokollt használ, például az X.21-et és a V.35-t. Ezek a protokollok rögzítik azokat a jel- kód- és elektronikus paramétereket, melyeket a forgalomirányítók és a CSU/DSU eszközök használnak az egymással való kommunikációhoz.



EIA/TIA-232

- Maximálisan 64 Kbit/s jelsebességet tesz lehetővé egy 25 érintkezős D csatlakozó segítségével, rövid távolságokra
- Korábban RS-232-nek nevezték
- Ugyanaz, mint az ITU-T V.24 specifikáció

EIA/TIA - 449/530

- Az EIA/TIA-232 gyorsabb változata (maximálisan 2 Mbit/s)
- 36 érintkezős D csatlakozót használ és hosszabb kábeles távolságok áthidalására képes
- RS-422 és RS-423 néven is ismert

EIA/TIA - 612/613

- Egészen 52 Mbit/s sebességig biztosít hozzáférést a szolgáltatásokhoz, egy 60 érintkezős D csatlakozó segítségével

V.35

- Egy ITU-T szabvány a szinkron kommunikációért egy hálózati hozzáférési eszköz és egy csomag-alapú hálózat között, egészen 48 Kbit/s sebességig
- 34 érintkezős téglalap alakú csatlakozót használ

X.21

- ITU-T szabvány a szinkron digitális kommunikációért
- 15 érintkezős csatlakozót használ

A technológiai fejlesztések egyre jobb jelzési szabványokat eredményeznek, amelyek megnövekedett sebességet, nagyobb adatforgalmat tesznek lehetővé.

A megfelelő WAN technológia kiválasztásakor fontos szempont a kapcsolat sebessége. A WAN-kapcsolatokat megvalósítására létrehozott első digitális hálózatok 64 kbit/s sebességű kapcsolatokat támogattak, bérelt vonalon keresztül. A 0-s szintű digitális csatorna (Digital Signal level 0, DS0) kifejezés erre a szabványra utal.

A technológia fejlődésével, a szolgáltatók a DS0 csatorna kibővített változatait is biztosították az előfizetők számára. Észak-Amerikában például a DS1 szabvány, más néven T1 vonal, egy olyan kommunikációs vonalat definiál, amely 24 DS0 adatcsatornát, és egy 8 kbit/s sebességű, jelzésrenszeri csatornát foglal magában. Ez a szabvány maximálisan 1,544 Mbit/s sebességet tesz lehetővé. A T3 vonalak a DS3 szabványt használják, amely 28 DS1 csatornát fog össze és ezáltal maximálisan 44,736 Mbit/s átviteli sebességre képes.

A világ más részein más szabványokat alkalmaznak. Európában például E1 vonalakat kínálnak a szolgáltatók, melyek 32 DS0 csatorna támogatásával 2,048 Mbit/s sebességre képesek. Találkozhatunk E3 kapcsolatokkal is, melyek 16 E1 vonalat felhasználva maximálisan 34,064 Mbit/s sebességet biztosítanak.

Vonal típusa	Jelzési szabvány	Bitsebesség
56	DS0	56 Kbit/s
64	DS0	64 Kbit/s
T1	DS1	1,544 Mbit/s
E1	ZM	2.048 Mbit/s
E3	M3	34.064 Mbit/s
J1	Y1	2.048 Mbit/s
T3	DS3	44736 Mbit/s
OC-1	SONET	51.84 Mbit/s
OC-3	SONET	155,54 Mbit/s
OC-9	SONET	466.56 Mbit/s
OC-12	SONET	622.08 Mbit/s
OC-18	SONET	933.12 Mbit/s
OC-24	SONET	1244.16 Mbit/s
OC-36	SONET	1866.24 Mbit/s
OC-48	SONET	2488.32 Mbit/s

7.1.2 WAN szabványok

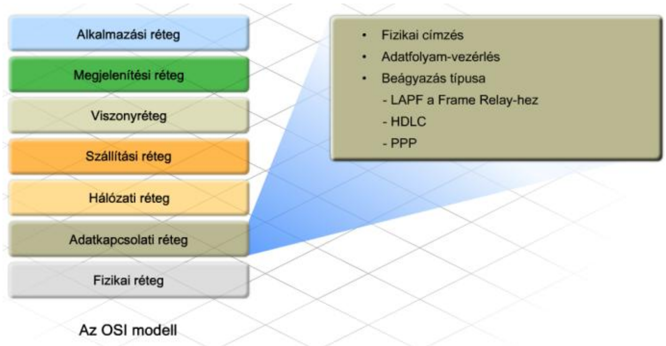
Az ide vonatkozó szabványokhoz igazodó hálózattervezés biztosítja, hogy a WAN környezetben előforduló összes eszköz és technológia együttműködhessen egymással.

A WAN szabványok az adatok szállításának fizikai- és adatkapcsolati rétegbeli jellemzőit specifikálják. Az adatkapcsolati rétegre vonatkozó WAN szabványok olyan paramétereket irnak elő, mint a fizikai címzés, az adatfolyamvezérlés (flow control) vagy a beágyazás típusa, de leirják az információ mozgatásának a WAN-kapcsolaton keresztüli megoldását is. Az alkalmazott WAN technológia típusa pontosan meghatározza a felhasznált adatkapcsolati rétegre vonatkozó szabványokat. Néhány példa 2. rétegbeli WAN protokollokra:

- Kapcsolatelérési eljárás Frame Relay-hez (Link Access Procedure for Frame Relay, LAPF)
- Magasszintű adatkapcsolat-vezérlés (High-level Data Link Control, HDLC)
- Pont-pont protokoll (Point-to-Point Protocol, PPP)

Számos szervezet van, amely a fizikai- és az adatkapcsolati rétegbeli WAN szabványok kezeléséért felelős. Ilyen szervezet például:

- Nemzetközi Telekommunikációs Szövetség Telekommunikációs Szabványosítási Csoportja (International Telecommunications Union Telecommunications Standardization Sector, ITU-T)
- Nemzetközi Szabványügyi Hivatal (International Organization for Standardization, ISO)
- Internet Mérnöki Munkacsoport (Internet Engineering Task Force, IETF)
- Elektronikai Iparágak Szövetsége (Electronics Industry Alliance, EIA)
- Telekommunikációs Ipari Szövetség (Telecommunications Industry Association, TIA)

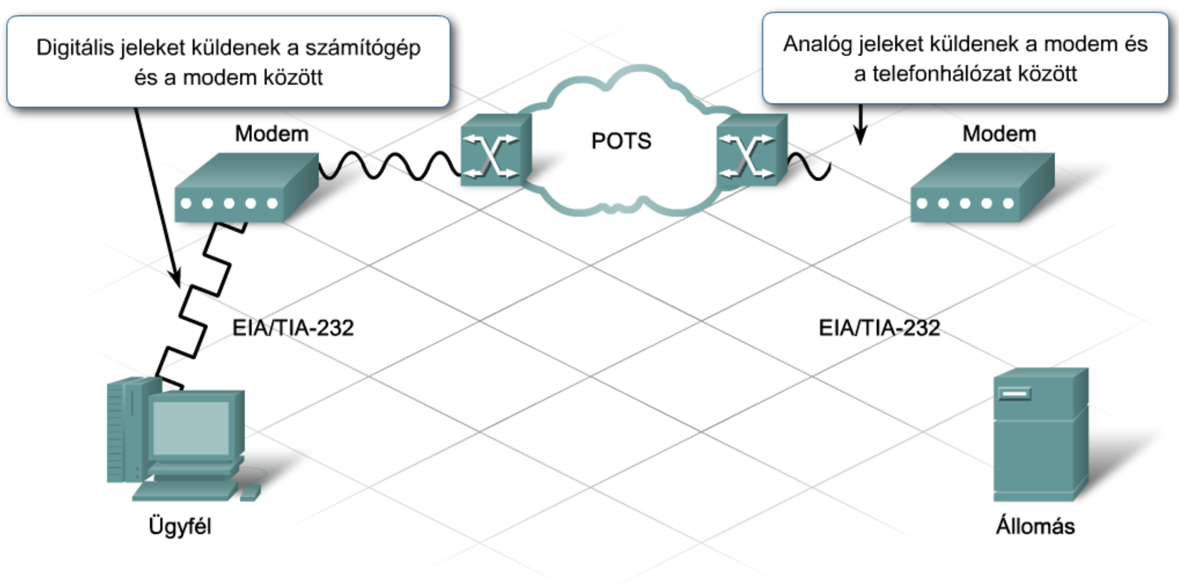


7.1.3 WAN-kapcsolatok létesítése

A WAN-kapcsolatok digitális vagy analóg technológiát használnak. Analóg kapcsolatok esetén az adatok kódolással, más néven modulálással kerülnek rá egy vivőhullámra. A modulált jel ezután továbbviszi az információkat az átviteli közegen a távoli végpont felé. A távoli helyen a jel demodulálásra kerül, és a vevőoldal kinyeri az információt.

Átvitel előtt a modem rákódolja az információt a vivőhullámra, a vevő oldalon pedig dekódolja azt. Nevét feladatáról kapta: a vivőjel modulálása és demodulálása (modem).

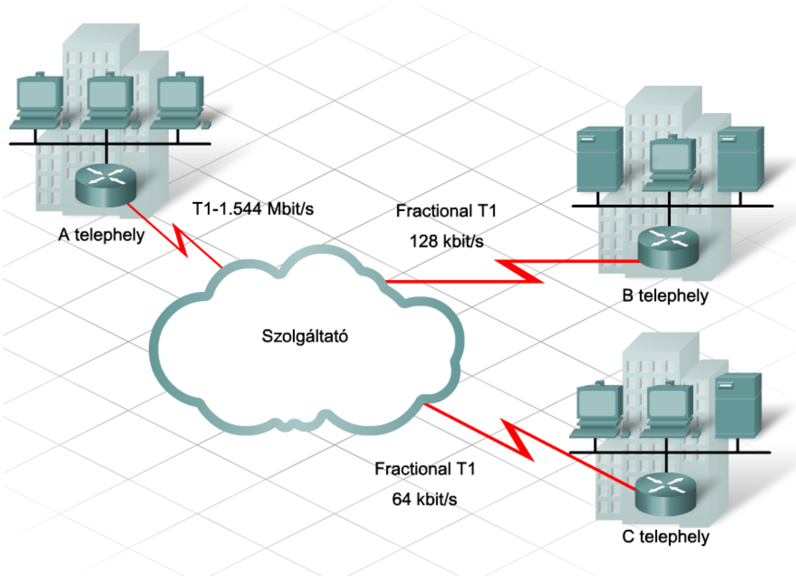
Modemek segítségével a távoli állomások a hagyományos telefon-rendszert (Plain Old Telephone System, POTS) használatáva kommunikálhatnak egymással. Ezen kívül a felhasználók digitális előfizetői vonalakon (Digital Subscriber Line, DSL) vagy kábeltelevíziós (Cable Television, CATV) kapcsolatokon is csatlakozhatnak a szolgáltatók hálózataihoz.



Számos vállalat fizet elő olyan szolgáltatásokra, amelyek dedikált vonalak segítségével biztosítják az összeköttetést telephelyük és az ISP között. Ezek gyakran bérelt vonali szolgáltatások formájában valósulnak meg, melyekért a vállalatok havi előfizetési díjat fizetnek. Ezek a vonalak óriási mennyiségű adat átvitelére képesek. Egy T1 kapcsolat például 1,544 Mbit/s, míg egy E1 vonal 2,048 Mbit/s sebességgel képes továbbítani a forgalmat. Gyakran ez a sávszélesség nagyobb, mint amire a szervezetnek valójában szüksége lenne. Egy T1 vonal felosztható 24 darab 64 Kbit/s sebességű DS0 csatornára. Ebben az esetben az ügyfél a T1/E1 kapcsolatnak csak egy részére, más néven részleges (frakcionális) T1 vagy E1 kapcsolatra fizet elő.

A nagy sávszélességű kapcsolatok több DS0 csatornára bonthatóak fel. Az internetszolgáltatók az egyes DS0 vonalakhoz különböző kommunikációs párbeszédeket vagy végfelhasználókat rendelhetnek hozzá. A szervezetek egy vagy több DS0 csatornát is megvásárolhatnak. Egy DS0 csatorna nem egy fizikailag különálló entitás, inkább a vonal fizikai sávszélességének egy időszeletéhez hasonlítható. Az egyes frakcionális kapcsolatok az összes időtartam egy töredékéig teljes hozzáférést tesznek lehetővé az átviteli közeghez a szervezet számára. Két technika létezik arra, hogy az idő függvényében az információküldéshez egyetlen kábel sávszélességét több csatorna

között lehessen megosztani: az egyszerű időosztásos multiplexelés (Time Division Multiplexing, TDM) és a statisztikai alapú időosztásos multiplexelés (Statistical-Time Division Multiplexing, STDM).



Az időosztásos multiplexelés (TDM) előre meghatározott időrések alapján osztja meg a sávszélességet. Minden ilyen időrést egy egyedi párbeszédhez rendelnek. Az egyes időrések azt az időtartamot reprezentálják, ami alatt egy párbeszéd teljes körűen használhatja a fizikai átviteli közeget. A sávszélességet attól függetlenül lefoglalják az egyes csatornák vagy időrések számára, hogy a csatornát használó állomásnak vannak-e továbbításra váró adatai. Következésképpen a szabványos TDM esetén, ha egy állomásnak éppen nincs küldendő üzenete, időrése kihasználatlan marad, elpazarolva az értékes sávszélességet.

A statisztikai időosztásos multiplexelés (STDM) hasonlít a TDM-hez, eltekintve attól, hogy nyomon követi a többlet sávszélességet igénylő párbeszéd-folyamokat. Ez a megoldás a fel nem használt időréseket az aktuális szükségletek szerint dinamikusan kiosztja. Ily módon az STDM segítségével minimalizálható az elpazarolt sávszélesség.

7.1.4 Csomag- és vonalkapcsolás

Egy nagyvállalat számtalan módon csatlakozhat WAN szolgáltatásokhoz.

Dedikált bérelt vonal

Az egyik kapcsolódási típus a pont-pont soros összeköttetés két forgalomirányító között, dedikált bérelt vonal segítségével. Ezzel végpont-végpontpont típusú kapcsolat hozható létre, mely alapvető adattovábbítási feladatok ellátására képes. Minden ilyen összeköttetés végpontonként egy különálló fizikai interfészt és egy külön CSU/DSU berendezést igényel. Ahogy egy szervezet egyre több telephelyet alakít ki, az egyes helyszínek közötti bérelt vonalak fenntartása nagyon költségessé válhat.

Vonalkapcsolás

Vonalkapcsolás esetén egy áramkör jön létre az állomások között, mielőtt azok bármilyen adatot továbbítanának. A szabványos telefonos hívások ezt a kapcsolódási típust használják. A vonalkapcsolás az áramkör bekapcsolt állapota alatt fix sávszélességet biztosít a két végpont között.

A párbeszéd befejeztével az áramkör felszabadul. Más szervezet nem használhatja az áramkört addig, amíg az szabaddá nem válik. Ez egyfajta biztonságot jelent, amely nincs jelen a csomagkapcsolt vagy a cellakapcsolt technológiák esetében.

Vonalkapcsolás esetén akkor rendelik hozzá a szolgáltatók az egyes kapcsolatokhoz az összeköttetéseket, amikor az erre vonatkozó igényt beérkezik. Költséget csak akkor számolnak fel, ha az összeköttetés használatban van. Egy vonalkapcsolt összeköttetés költsége a használati idő függvényében változik, és gyakori használat esetén meglehetősen drága lehet.

Csomagkapcsolás

A csomagkapcsolás jóval hatékonyabban használja ki a vonalak sávszélességét, mint más kapcsolási típusok. Az adatokat itt csomagokra bontják, melyekhez cél- és forrás-azonosítókat rendelnek. Ezután az adatok a szolgáltató hálózatába lépnek. A szolgáltató fogadja az adatokat és célcimük alapján továbbkapcsolja azokat egyik csomópontról a másikra, míg el nem érik végső céljukat. A forrás és cél közötti útvonal vagy áramkör, általában előre meghatározott, de nem kizárólagos használatú összeköttetés. A szolgáltatók a különböző szervezetek felől érkező csomagokat ugyanazon összeköttetéseken keresztül kapcsolják. A csomagkapcsolt technológia egyik példája a Frame Relay.

Cellakapcsolás

A cellakapcsolás a csomagkapcsolás egy változata. Alkalmas hang, video és adatátvitelre magán vagy nyilvános hálózatokon keresztül, akár 155 Mbit/s sebességgel. Az ATM (Asynchronous Transfer Mode) technológia fix méretű, 53 bájtos cellákat használ, melyek egy 48 bájtos adatrészből és egy 5 bájtos fejrészből állnak. A kicsi, egyforma méretű cellák gyors és hatékony kapcsolást tesznek lehetővé a csomópontok között. Az ATM technológia egyik előnye, hogy megakadályozza, hogy a kisebb méretű üzeneteket visszatartsák a nagyobb méretű üzenetek. A főként szegmentált adatokat forgalmazó hálózatokban azonban az ATM nagymértékű többletterhelést eredményez, amely ténylegesen csökkenti a hálózat teljesítményét.

Virtuális áramkörök

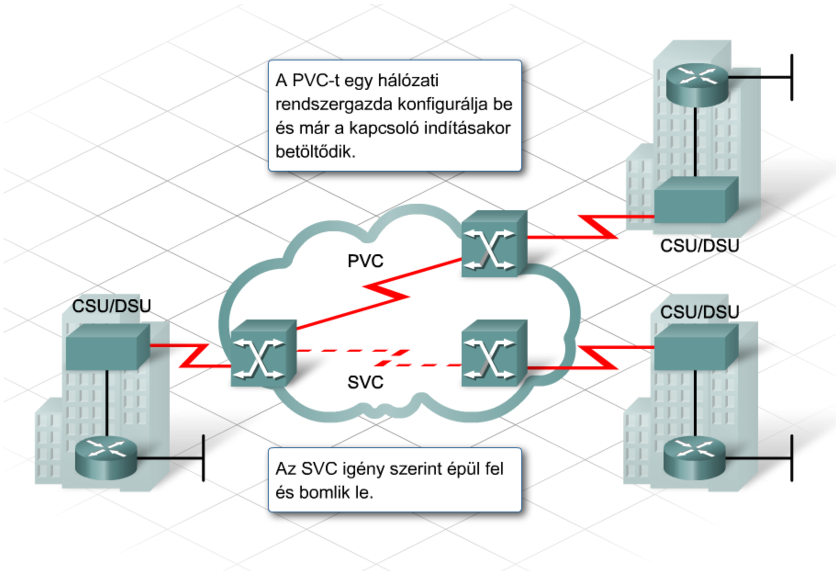
Csomagkapcsolt technológia használata során a szolgáltató virtuális áramköröket (Virtual Circuit, VC) hoz létre. Egy virtuális áramkör az egyes csomagkapcsoló eszközök közötti összeköttetéseket a különböző forrásból származó csomagok között megosztva használja. Ennek eredményeképpen, az átviteli közeg nem kerül kizárólagos használat alá a kapcsolat időtartama alatt. Kétféle virtuális áramkör létezik: kapcsolt és állandó.

Kapcsolt virtuális áramkörök

A kapcsolt virtuális áramkörök (Switched, SVC) dinamikusan jönnek létre két végpont között, amikor egy forgalomirányító adatot kíván továbbítani. Az áramkör igény szerint épül fel, és lebomlik miután az átvitel befejeződött, (például letöltődött egy állomány). Egy SVC létrejöttekor hívásfelépítési információkat kell elküldeni mielőtt bármilyen adatot küldhető. A hívásbontási információk megszakítják a kapcsolatot, ha arra már nincs szükség. Ez a folyamat némi késleltetést eredményez a hálózatban, mivel minden párbeszéd esetén fel kell építeni majd le kell bontani a virtuális áramköröket.

Állandó virtuális áramkörök

Az állandó virtuális áramkörök (Permanent, PVC) tartós útvonalat biztosítanak két pont között az adatok továbbításához. A szolgáltatónak előre be kell állítania a PVC-ket, melyek nagyon ritkán bomlanak fel vagy kapcsolódnak szét. Ez a tulajdonság szükségtelenné teszi a hívások felépítését, illetve lebontását, és ennek köszönhetően felgyorsul az információáramlás a WAN-kapcsolaton keresztül. A PVC-k segítségével a szolgáltatók sokkal nagyobb mértékben képesek kézben tartani a hálózat adatáramlási mintáit és a felügyeleti feladatokat. A PVC-k népszerűbbek az SVC-knél, és gyakran olyan telephelyek kiszolgálására használják őket, amelyek állandó, nagyméretű adatforgalmat bonyolítanak. A Frame Relay jellemzően PVC-ket használ.



7.1.5 Helyi hurok és nagytávolságú WAN technológiák

Az ISP-k többfajta WAN technológiát használnak ügyfeleik csatlakoztatásához. Az a kapcsolódási típus, melyet a helyi hurok, vagy más néven „utolsó mérföld” (last mile) esetében használnak, nem feltétlenül egyezik meg azzal a WAN kapcsolódási típussal, amit az ISP hálózatán belül vagy a különböző szolgáltatók között alkalmaznak.

Helyi huroknál alkalmazott technológiák például a következők:

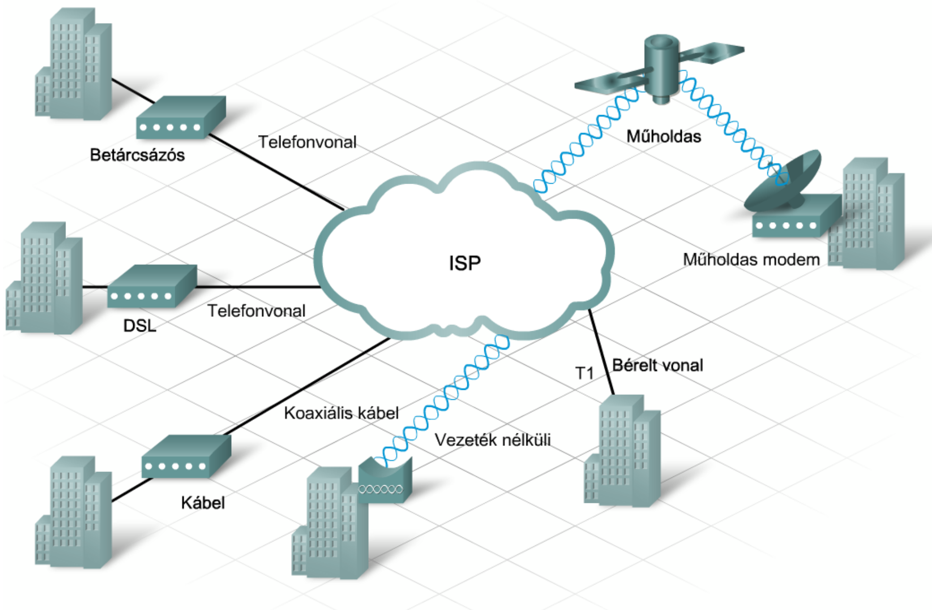
- analóg betárcsázás
- integrált digitális hálózat (Integrated Services Digital Network, ISDN)
- bérelt vonal
- kábeltévés kapcsolat
- digitális előfizetői vonal (Digital Subscriber Line, DSL)
- Frame Relay
- vezeték nélküli kapcsolat

Ezen technológiák mindegyike biztosít előnyöket és hátrányokat egyaránt az előfizetők számára. Nem minden földrajzi területen érhető el az összes itt felsorolt technológia.

Amikor egy szolgáltató adatokat fogad, továbbítania kell azokat a távoli végpontok felé, hogy végül eljussanak a címzetthez. Ezek a távoli helyek tartozhatnak az ISP hálózatához vagy képezhetik a

különböző internetszolgáltatók közötti szakaszokat. Nagytávolságú kommunikációs kapcsolatokkal gyakran találkozhatunk az internetszolgáltatók között vagy óriásvállalatok fiókirodáinak összeköttetése esetén.

Sok különböző WAN technológia áll rendelkezésre a szolgáltatók számára, amelyek nagy távolságok esetén is lehetővé teszik a megbízható adattovábbítást. Ezek közé tartoznak például az ATM, a Frame Relay, a műholdas- és a bérelt vonalas kapcsolatok.



A nagyvállalatok folyamatos növekedése növekvő számú, a világ legkülönbözőbb területein létrejövő telephelyet eredményeznek. Ennek eredményeképpen az alkalmazásoknak egyre nagyobb és nagyobb sávszélességre van szükségük. Ez a növekedés olyan nagysebességű és nagy sávszélességű technológiát igényel, ami alkalmas nagyobb távolságra történő adattovábbításra is.

A Szinkron Optikai hálózat (Synchronous Optical Network, SONET) és a Szinkron Digitális Hierarchia (Synchronous Digital Hierarchy, SDH) olyan szabványok, melyek nagy mennyiségű adat átvitelét biztosítják, nagy hatótávolsággal rendelkeznek, és optikai kábeleket használnak. Mind a SONET, mind az SDH magában foglalja a korai digitális átviteli szabványokat, és támogatja az ATM, illetve a Packet over SONET/SDH (POS) hálózatokat. Mindkét technológiát használják adatok és hangüzenetek továbbítására is.

A DWDM (Dense Wavelength Division Multiplexing) az egyik olyan új fejlesztés, amely támogatja a rendkívül nagy távolságú adatkommunikációt. A DWDM a beérkező optikai jelekhez meghatározott frekvenciájú vagy hullámhosszú fényt rendel hozzá. Képes e hullámhosszok erősítésére is, ami fokozza a jelerősséget. A DWDM több mint 80 különböző hullámhossz vagy adatcsatorna egyetlen üvegszálra történő multiplexelésére ad



lehetőséget. Az egyes csatornák 2,5 Gbit/s sebességen képesek átvinni a multiplexelt jeleket.

Az adat vevő oldalon történő demultiplexelése lehetőséget ad több különböző adatfolyam egyetlen optikai szálon történő átvitelére, akár eltérő adatátviteli sebességek használatával is. A DWDM például képes IP, SONET és ATM formátumú adatok egyidejű átvitelére.

7.2 Gyakori WAN beágyazások összehasonlítása

7.2.1 Ethernet és WAN beágyazások

A beágyazási folyamat még azelőtt lezajlik, mielőtt az adatok áthaladnak a WAN-kapcsolaton. A beágyazás egy olyan konkrét formátumhoz illeszkedik, amely a hálózaton használt technológián alapszik. Mielőtt az adatokat bitekké alakítanák a közegen való átvitelhez, a 2. rétegbeli beágyazási folyamatcímzési és vezérlési információkat ad az adatokhoz.

A 2. réteg a fizikai hálózati átvitel típusára jellemző fejléc információkat ad hozzá az adatokhoz. LAN környezetben az Ethernet a leggyakrabban előforduló technológia. Az adatkapcsolati réteg Ethernet keretekbe ágyazza a csomagokat. A keret fejlécek olyan információkat tartalmaznak, mint a forrás és cél MAC-címek, és olyan Ethernetre jellemző vezérlőket, mint a keretméret és az időzítési információk.

Hasonlóképpen az előbbiekhez, a WAN-kapcsolatokon való átvitelre szánt keretek beágyazása illeszkedik az összeköttetésen használatban lévő technológiával. Ha egy összeköttetés például Frame Relay-t használ, akkor Frame Relay specifikus beágyazási típusra van szükség.

Az adatkapcsolati rétegbeli beágyazás típusa elkülönül a hálózati réteg beágyazási típusától. Ahogy az adatok áramlanak a hálózaton keresztül, az adatkapcsolati rétegbeli beágyazás típusa folyamatosan változhat, míg a hálózati rétegbeli beágyazás mindvégig változatlan marad. Ha egy csomag a célállomás eléréséhez áthalad egy WAN-kapcsolaton, a 2. rétegbeli beágyazás típusa a kapcsolatot megvalósító WAN technológiához igazodik.

A csomagok a helyi hálózatokból az alapértelmezett átjáró szerepét betöltő forgalomirányítón keresztül jutnak ki. A forgalomirányító eltávolítja az Ethernet keret információit majd a WAN-kapcsolatnak megfelelő új keretbe ágyazza az adatokat. A WAN interfészen fogadott adatok Ethernet keretformátumra történő átalakítása azelőtt megy végbe, hogy azokat a helyi hálózatra helyeznék. A forgalomirányító átviteli közeg átalakítóként szolgál (média konverter), mivel az adatkapcsolati rétegbeli keretformátumot az interfésznek megfelelően változtatja meg.

Pont-pont kapcsolatok esetén a beágyazási típusnak mindkét oldalon meg kell egyeznie. Az adatkapcsolat rétegbeli beágyazási típusok a következő adatmezőket tartalmazzák:

Jelző (flag)

- Az egyes keretek kezdetét és végét jelöli meg.

Cím

- A beágyazás típusától függ.
- Nem szükséges a pont-pont WAN-kapcsolatoknál.

Vezérlés

- A keret típusának jelzésére szolgál.

Protokoll

- A beágyazott hálózati rétegbeli protokoll megadására használják.
- Nem szerepel minden WAN beágyazási típus esetén.

Adat

- rétegbeli adatot és az IP adategységet foglalja magába.

Keretellenőrző sorozat (FCS)

- Ellenőrzési mechanizmust biztosít annak megállapításához, hogy nem sérült-e meg a keret átvitel közben.

7.2.2 HDLC és PPP

A HDLC és a PPP a két leggyakoribb soros vonali 2. rétegbeli beágyazási típus.

A HDLC (High-level Data Link Control) szabványos, bit-orientált adatkapcsolati rétegbeli beágyazási típus. A HDLC szinkron soros átvitelt használ, mely hibamentes kommunikációt biztosít két pont között. A HDLC protokoll definiál egy 2. rétegbeli keretszervezési (frame) struktúrát, amely nyugtázás és ablakozási rendszer használatával áramlásvezérlésre és hibakezelésre ad lehetőséget. Minden keret ugyanolyan formátumú, akár adatkeretről, akár vezérlőkeretről legyen szó.

A szabványos HDLC keretformátum nem tartalmaz olyan adatmezőt, amely azonosítaná a keret által hordozott protokoll típusát. A szabványos HDLC emiatt nem képes többfajta protokoll átvitelére ugyanazon az összeköttetésen keresztül.

A Cisco HDLC protokoll bevezet egy további adatmezőt, amely típus (Type) néven ismert. Segítségével lehetőség nyílik arra, hogy több hálózati rétegbeli protokoll megosztva használja ugyanazt a kapcsolatot. Csak akkor használjuk a Cisco HDLC protokollt, ha Cisco készülékeket szeretnénk összekapcsolni egymással. A Cisco HDLC az alapértelmezett adatkapcsolati protokoll a Cisco soros kapcsolatoknál.

Nyílt szabványú HDLC keret

Jelző	Cím	Vezérlés	Információ	Keret-ellenőrző összeg	Jelző
8 bit	8 bit	8 vagy 16 bit	Változó hossz, 0 vagy több bit, 8 többszöröse	16 vagy 32 bit	8 bit

Cisco HDLC keret

Jelző	Cím	Vezérlés	Típus (Protokoll kód)	Információ	Keret-ellenőrző összeg	Jelző
8 bit	8 bit	8 bit	16 bit	Változó hossz, 0 vagy több bit, 8 többszöröse	16 bit	8 bit

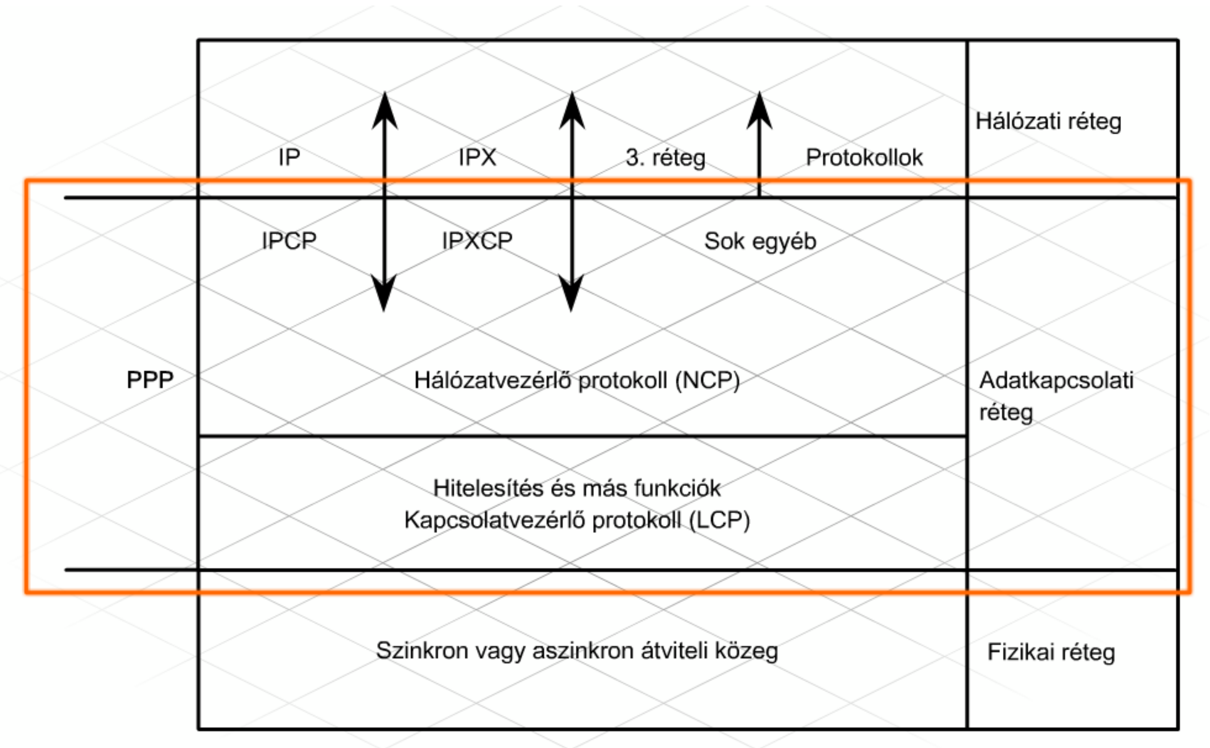
A HDLC-hez hasonlóan a Pont-Pont Protokoll (PPP) is soros összeköttetések számára készült adatkapcsolat rétegbeli beágyazási típus. Réteges felépítést használ, mely segítségével képes multi-protokoll adatcsomagok beágyazására és átvitelére pont-pont kapcsolatokon keresztül. Mivel a PPP protokoll szabványokon alapul, lehetővé teszi a kommunikációt a különböző gyártótól származó készülékek között.

A PPP a következő interfészeket támogatja:

- aszinkron soros
- szinkron soros
- HSSI (High-Speed Serial Interface)
- ISDN (Integrated Services Digital Network)

A PPP két alprotokollal rendelkezik:

- Kapcsolatvezérlő protokoll (Link Control Protocol, LCP) – a pont-pont kapcsolatok felépítéséért, fenntartásáért és lebontásáért felelős.
- Hálózatvezérlő protokoll (Network Control Protocol, NCP) – együttműködést biztosít a különböző hálózat rétegbeli protokollokkal.



Kapcsolatvezérlő protokoll

A PPP az LCP-t használja pont-pont összeköttetések kialakítására, fenntartására, tesztelésére és befejezésére. Az LCP észleli és konfigurálja a WAN-kapcsolat vezérlő-beállításait. Néhány beállítási lehetőség, amiket az LCP kezel:

- hitelesítés (authentication)
- tömörítés

- hibafelismerés
- több kapcsolat (multilink)
- PPP visszahívás

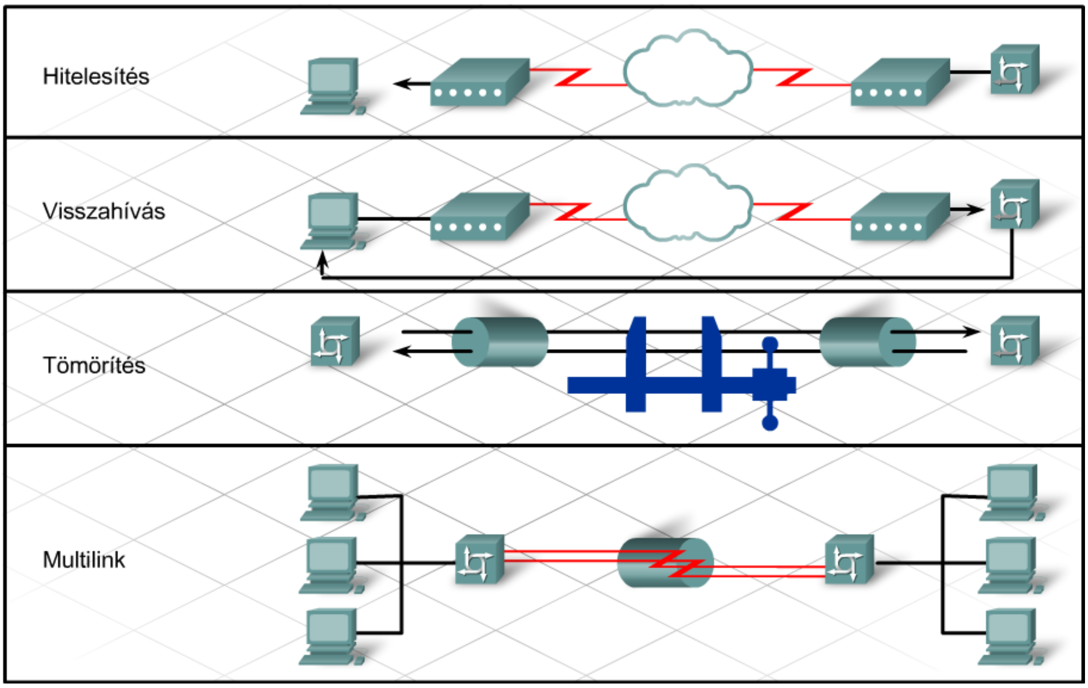
A fentieken túl az LCP a következőkért felelős:

- kezeli a különböző méretű csomagokat
- észleli a gyakori konfigurációs hibákat
- képes a jól és a hibásan működő kapcsolatok megkülönböztetésére

Hálózatvezérlő protokoll (NCP)

A PPP az NCP-t használja a különböző hálózat rétegbeli protokollok beágyazására, így azok képesek ugyanazon kommunikációs kapcsolaton keresztül működni.

A PPP kapcsolatokon használt minden hálózati protokolloknak saját hálózatvezérlő protokollra van szüksége. Az internetprotokoll (IP) például, az IP vezérlőprotokollt (IPCP), az IPX pedig az IPX vezérlőprotokollt (IPXCP) használja. Az NCP-k a beágyazott hálózati rétegbeli protokollok azonositására jelzőkódokat tartalmazó adatmezőket használnak.



Hitelesítés

Hitelesítési lehetőségek segítségével az összeköttetés hívó felének meg kell adni a megfelelő információkat, így biztosítható, hogy a hívó rendelkezzen jogosultságokkal a hívás lebonyolításához. Az összeköttetés két végén levő forgalomirányítók hitelesítési üzeneteket küldenek egymásnak. Két lehetséges megoldás a hitelesítés elvégzésére a jelszó-hitelesítő protokoll (PAP) és a kihívásos kézfogás hitelesítési protokoll (CHAP) használata.

Visszahívás

Ezzel az LCP-funkcióval a Cisco forgalomirányítók visszahívási ügyfélként és visszahívási kiszolgálóként egyaránt működhetnek. Visszahívásnál az ügyfél egy hívással létrehozza a kezdeti kapcsolatot, kéri a kiszolgálótól a visszahívását, majd megszakítja a kapcsolatot. A visszahívó forgalomirányító válaszol az első hívásra, és a konfigurációjában megadottak alapján visszahívja az ügyfelet.

Tömörítés

A tömörítési funkció a keretekben továbbítandó adatok mennyiségének csökkentésével, a PPP-kapcsolat átviteli sebességének növelésére használható. A keretek kibontását a túloldalon a protokoll végzi. A Cisco forgalomirányítók két tömörítő protokollt ismernek, ezek a Stacker és a Predictor.

Multilink

Ez a lehetőség terheléselosztást biztosít a PPP forgalomirányító interfészek között.

A PPP-kapcsolatok létrehozásának folyamata három fázisra bontható, ezek az összeköttetés létrehozása, a hitelesítés (ez elhagyható) és a hálózati rétegbeli protokoll használatának fázisa.

Az összeköttetés létrehozása

A PPP LCP-kereteket küld az adatkapcsolat konfigurálása és tesztelése céljából. Az LCP-keretek tartalmaznak egy konfigurációs mezőt, amely lehetővé teszi például a maximális átviteli egység (Maximum Transmission Unit, MTU) méretének, a tömörítésnek és a kapcsolat hitelesítésének egyeztetését. Ha egy LCP-keretből hiányzik valamelyik konfigurációs beállítás, a hiányzó konfigurációs elemhez a protokoll az alapértelmezett értéket rendeli hozzá. A kapcsolat hitelesítési típusának meghatározása és az átviteli minőség tesztelése elhagyható paramétereknek számítanak az összeköttetés létrehozása során. A kapcsolat minőségének meghatározásával eldönthető, hogy az összeköttetés megfelelő-e a hálózati rétegbeli protokollok használatához. A fentebb említett elhagyható konfigurációs paraméterek beállításának meg kell történni, mielőtt az eszközök fogadnák a konfiguráció helyességét igazoló nyugtát. Ez a fázis akkor tekinthető befejezettnek, ha a végponti készülékek megkapták a konfigurációt nyugtázó keretet.

Hitelesítési fázis (elhagyható)

A hitelesítési fázis jelszavas védelmet biztosít a kapcsolódó végpontok (például forgalomirányítók) azonosításához. A hitelesítésre a forgalomirányítók paramétereinek elfogadása után kerül sor, de még azelőtt, hogy az NCP egyeztetési fázis megkezdődne.

NCP egyeztetési fázis

A PPP végpont NCP csomagokat küld, melyekkel egy vagy több hálózati rétegbeli protokollt (például, az IP-t vagy az IPX-et) választ ki és konfigurál. Amikor az LCP bontja a kapcsolatot, értesíti a hálózati rétegbeli protokollokat, így azok végrehajthatják a megfelelő műveletet. A `show interfaces` parancs megmutatja az LCP és NCP állapotokat.

Ha a PPP kapcsolat létrejött, mindaddig aktív marad, amíg az LCP vagy az NCP fel nem bontja a kapcsolatot, vagy le nem jár egy aktivitást figyelő számláló. A felhasználók is kezdeményezhetik a kapcsolat befejezését.

7.2.3A PPP konfigurálása

A Cisco forgalomirányítók soros interfészein a HDLC az alapértelemezett beágyazási típus. A beágyazás típusának megváltoztatásához, valamint a PPP sajátosságainak használatához használja a következő parancsot:

```
encapsulation ppp
```

- Ez aktiválja a PPP beágyazást a soros interfészen.

Miután a PPP engedélyezésre került, beállíthatóvá válnak az opcionális paraméterek, például a tömörítés és a terheléselosztás.

```
compress [predictor | stac]
```

- Engedélyezi a tömörítést az interfészen, predictor (előjósló) vagy stacker (verem-tárolásos) módszer használatával.

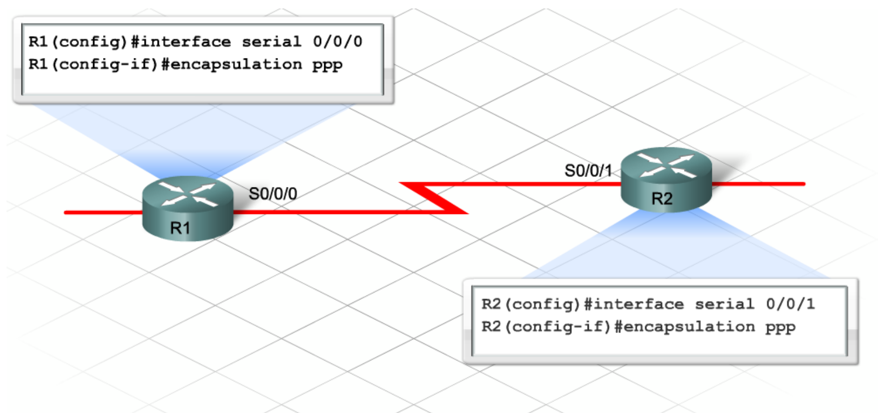
```
ppp multilink
```

- Segítségével terheléselosztás konfigurálható több összeköttetés között.

A hálózaton átküldött adatok tömörítése javíthatja a hálózat teljesítményét. A predictor és stacker szoftveres tömörítési technikák, amelyek tömörítési módjukban térnek el egymástól. A stacker processzorigényesebb tömörítés, de kevesebb memóriára van szüksége, a predictor technika viszont kevésbé terheli a processzort, de több memóriát használ. Ezért a stacker-t akkor érdemes használni, ha a vonal sávszélessége a szűk keresztmetszet, a predictor-t pedig abban az esetben, ha a forgalomirányító túlterhelt.

Csak akkor engedélyezzük a tömörítést, ha a hálózat teljesítménye megkívánja azt, mivel használata növeli a forgalomirányító feldolgozási idejét és többletterhelést okoz. Abban az esetben sem érdemes tömörítést alkalmazni, ha a hálózat forgalmát képező adatok döntő többsége már egyébként is tömörített állományokból áll. Egy tömörített fájl újbóli tömörítése többnyire méretnövekedéssel jár.

A PPP multilink több WAN összeköttetés egyetlen logikai csatornává történő összevonását teszi lehetővé. Ez terhelésmegosztást eredményez különböző kapcsolatok között, és bizonyos szintű biztonságot jelent abban az esetben, ha valamelyik összeköttetés meghibásodna.



Alapvető PPP konfiguráció

Az alábbi parancsokat HDLC és PPP beágyazások konfigurációinak ellenőrzéséhez és hibaelhárításához használják.

`show interfaces serial`

- Megjeleníti a beágyazás típusát és a kapcsolatvezérlő protokoll (LCP) állapotait.

`show controllers`

- Kijelzi az interfész-csatornák állapotát és azt, hogy csatlakozik-e kábel az interfészhez.

`debug serial interface`

- Segítségével ellenőrizhető az ébrenléti (keepalive) üzenetek számának folyamatos növekedése. Ha ezeknek a csomagoknak a száma nem növekszik, akkor valószínűleg időzítési probléma lépett fel az interfészkártyában vagy a hálózatban.

`debug ppp`

- Információt biztosít a PPP protokoll működési folyamatának különböző szakaszairól, beleértve az egyeztetést és a hitelesítést.

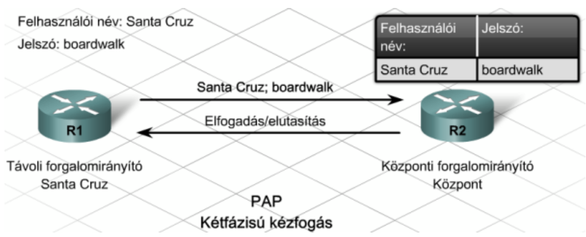
7.2.4 PPP hitelesítés

A PPP összeköttetések hitelesítésének beállítása elhagyható. Ha be van állítva, a hitelesítési folyamat közvetlenül a kapcsolat létrehozása után, de még a hálózati rétegbeli protokollok konfigurációs fázisa előtt lezajlik. A PPP összeköttetések két lehetséges hitelesítési típusa a jelszó hitelesítő protokoll (Password Authentication Protocol, PAP), illetve a kihívásos kézfogás hitelesítési protokoll (Challenge Handshake Authentication Protocol, CHAP).

A PAP egyszerű eljárást biztosít a távoli állomás azonosításához. Kétfázisú (kétutas, két üzenetből álló) kézfogást használ a felhasználói név és a jelszó elküldéséhez. A hívott eszköz megvizsgálja a kezdeményező eszköz felhasználói nevét, majd meggyőződik arról, hogy a fogadott jelszó megegyezik-e az adatbázisában találhatóval. Ha a két jelszó megegyezik, a hitelesítés sikeres.

A PAP nyílt szöveges formátumban egymás után ismételve mindaddig elküldi a hálózaton a felhasználónév/jelszó párt, míg nyugta nem érkezik a hitelesítésről vagy le nem zárul a kapcsolat. Ez a hitelesítési mód nem biztosít védelmet a felhasználói név és jelszó csomaglehallgató program segítségével történő ellopása ellen.

További probléma forrása lehet, hogy a távoli állomás felel a bejelentkezési kísérletek gyakoriságának szabályozásáért és ütemezéséért. Miután a távoli állomás hitelesítése megtörtént, az a továbbiakban nem lesz újraellenőrizve. A folyamatos ellenőrzés hiányában az összeköttetés védtelen a hitelesített kapcsolat ellopásával (hijacking), illetve a forgalomirányítóhoz jogtalanul hitelesített hozzáférést eredményező visszajátszásos támadásokkal szemben.



A másik PPP hitelesítési módszer a kihívásos kézfogás hitelesítési protokoll (CHAP).

A kihívásos kézfogás hitelesítési protokoll

A CHAP sokkal biztonságosabb hitelesítési folyamat, mint a PAP. A CHAP nem küldi el a jelszót az összeköttetésen keresztül. A CHAP alapú hitelesítés az összeköttetés felépítésekor történik meg először, majd annak lebontásáig újra és újra megismétlődik. Itt a hívott eszköz felel a hitelesítés gyakoriságának szabályozásáért és ütemezéséért, ami eléggé valószínűtlenné teszi a jelszólopáson alapuló támadások sikerességét.

A CHAP háromutas kézfogást használ.

1. A PPP-összeköttetés létrehozásának fázisa megtörténik.

2. A helyi forgalomirányító kihívó (challange) üzenetet küld a távoli forgalomirányítónak.

A távoli forgalomirányító a kapott kihívó üzenet és a megosztott titkos kulcs segítségével, egyirányú hash függvény felhasználásával egy kivonatot hoz létre.

4. Ezután a kivonatot visszaküldi a helyi fogalomirányítónak.

5. A helyi forgalomirányító összeveti az érkezett választ a saját maga által számított kivonattal, melyet a kihívó üzenet és ugyanazon megosztott titkos jelszó valamint ugyanazon egyirányú hash függvény felhasználásával határoz meg.

6. Ha a két számított érték megegyezik, a helyi forgalomirányító nyugtázza a hitelesítést.

7. Abban az esetben, ha a két érték nem egyezik meg, a helyi forgalomirányító bontja a kapcsolatot.

A CHAP a kihívó üzenetek értékének megváltoztatásával biztosít védelmet a visszajátszásos támadásokkal szemben. Mivel a kihívó üzenet értéke egyedi és véletlenszerű, ezért az ebből számított kivonat (hash) értéke is egyedi és véletlenszerű lesz. Az ismételt kihívások használata csökkenti azt az időtartamot, amíg veszélynek van kitéve a kapcsolat. A helyi forgalomirányító vagy egy külső hitelesítési kiszolgáló felel a kihívó üzenetek gyakoriságának és ütemezésének szabályozásáért.

7.2.5 PAP és CHAP konfigurálása

PPP kapcsolatok hitelesítésének beállításához a következő globális konfigurációs parancsok használhatóak:

```
username név password jelszó
```

- Globális konfigurációs parancs.
- Létrehoz egy helyi adatbázist, amely a távoli eszköz felhasználói nevét és jelszavát tartalmazza.
- A felhasználói névnek pontosan meg kell egyeznie a távoli forgalomirányító állomásnevével. Ez a név érzékeny a kis- és nagybetűkre.

```
ppp authentication {chap | chap pap | pap chap | pap}
```

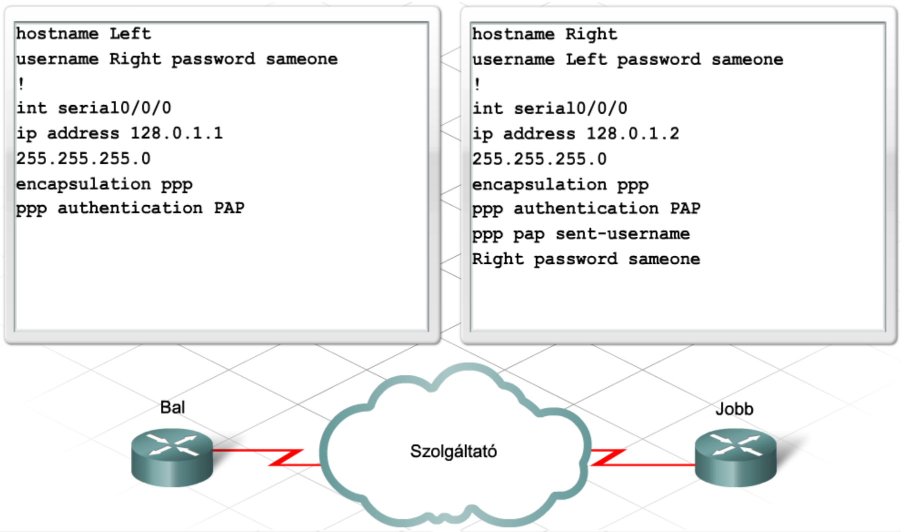
- Interfészkonfigurációs parancs.

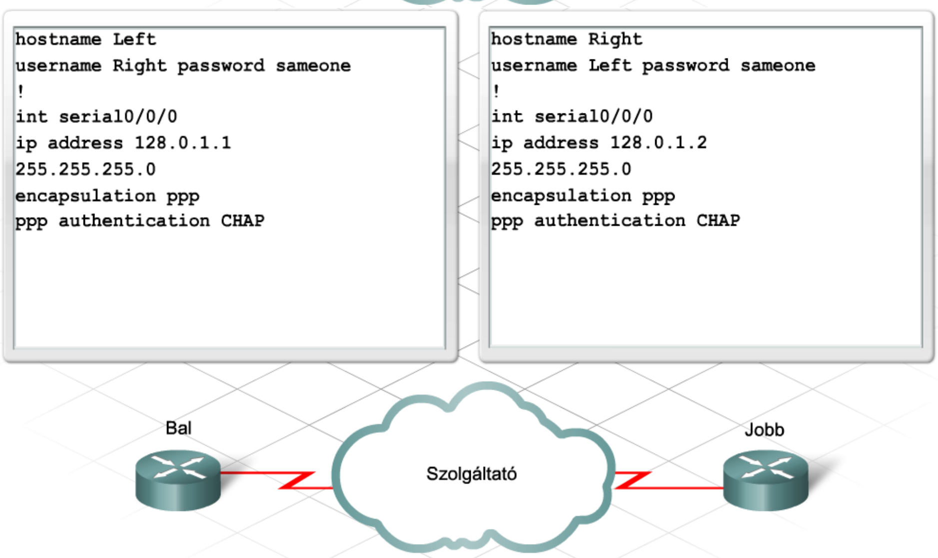
- Segítségével megadható az egyes interfészek által alkalmazott PPP hitelesítés típusa (PAP vagy CHAP).
- Ha egynél több hitelesítési típust állítottak be, például, chap pap, akkor a forgalomirányító először az első típussal próbálkozik és csak akkor fog próbálkozni a második módszerrel, ha arra a távoli forgalomirányító kéri.

A CHAP hitelesítés beállításához nincs szükség további konfigurációs parancsokra. Érdemes tudni, hogy a Cisco IOS 11.1 verziójától kezdődően alapértelmezés szerint a PAP le van tiltva az interfészeken. Ez azt jelenti, hogy a forgalomirányító akkor sem fogja elküldeni saját felhasználói név/jelszó értékeit, ha a PAP hitelesítés engedélyezett. A PAP használatához további parancsok szükségesek.

```
ppp pap sent-username név password jelszó
```

- Interfészkonfigurációs parancs.
- A távoli forgalomirányítónak küldendő felhasználói név/jelszó kombináció adható meg vele.
- Ennek meg kell egyeznie a távoli forgalomirányító helyi adatbázisában beállított felhasználói névvel és jelszóval.





A konfigurált kétutas hitelesítés segítségével az egyik forgalomirányító hitelesíti a másikat. Ha mindkét forgalomirányítón használjuk a debug parancsokat, akkor a hitelesítési folyamat alatt figyelhető meg az üzenetcsere forgalma.

debug ppp *{authentication | packet | error | negotiation | chap }*

Authentication (hitelesítés)

Megjeleníti a hitelesítési üzenetek sorozatát.

Packet (csomag)

Megjeleníti az összes küldött és fogadott PPP csomagot.

Negotiation (egyeztetés, tárgyalás)

Megjeleníti a PPP protokoll indulásakor továbbított, a PPP beállítások egyeztetéséért felelős csomagokat.

Error (hiba)

Protokollhibákat és statisztikai adatokat jelenít meg a PPP kapcsolatra és egyeztetésre vonatkozóan.

CHAP (kihívó üzenetek)

Megjeleníti az egymással váltott CHAP csomagokat.

A hibakeresést az egyes parancsok „no” előtaggal kiegészített változatával állíthatjuk le.

7.3 Frame Relay

7.3.1 A Frame Relay áttekintése

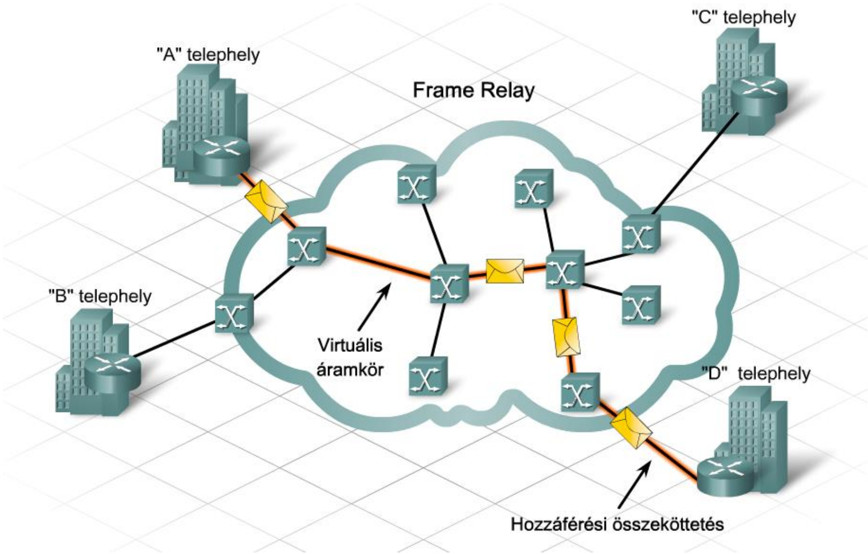
A Frame Relay egy gyakran előforduló 2. rétegbeli WAN beágyazási típus. A Frame Relay hálózatok többszörös hozzáférésűek, hasonlóan az Ethernethez, viszont az Ethernettől eltérően nem továbbítják a szórásos (broadcast) forgalmat. A Frame Relay hálózatok a nem szórásos többszörös hozzáférésű hálózatok közé tartoznak (NonBroadcast Multi-Access network, NBMA).

A Frame Relay változó hosszúságú csomagokat és csomagkapcsolási technológiát használ. Ez a protokoll is szinkron, időosztásos multiplexelést használ, a rendelkezésre álló vonali sávszélesség optimális kihasználásához.

A forgalomirányító (DTE) általában bérelt vonal segítségével áll összeköttetésben a szolgáltatóval. Ez a vonal egy Frame Relay kapcsolón (DCE) keresztül csatlakozik a szolgáltató legközelebb eső kapcsolódási pontjához (POP). Ezt a kapcsolatot nevezzük hozzáférési összeköttetésnek.

A célhálózathoz tartozó távoli forgalomirányító is DTE eszköz. A két DTE eszköz közötti kapcsolatot virtuális áramkörnek nevezzük (VC).

A virtuális áramkörök jellemzően a szolgáltató által előre konfigurált PVC-k segítségével jönnek létre. A legtöbb ISP nem javasolja vagy nem is teszi lehetővé a Frame Relay hálózatokban az SVC-k használatát.



7.3.2 A Frame Rekay működése

Az NMBA hálózatokban minden virtuális áramkörnek szüksége van 2. rétegbeli címre az azonosításhoz. Frame Relaynél ez a cím az adatkapcsolati azonosító (Data-Link Connection Identifier, DLCI).

A DLCI azonosítja a virtuális áramkört, amelyet az adatok használnak egy bizonyos célállomás eléréséhez. A DLCI minden továbbított keret címmezőjében megtalálható. A DLCI-nek általában csak helyi jelentősége van, és ugyanazon virtuális áramkör két végén eltérő DLCI is szerepelhet.

A 2. rétegbeli DLCI kapcsolatban van a virtuális áramkör másik végén lévő eszköz 3. rétegbeli címével. A DLCI összerendelése a távoli IP-címmel történhet statikusan, illetve dinamikusan is, az inverz ARP-ként ismert folyamat segítségével.

A DLCI azonosító távoli IP-címmel történő összerendelésének folyamata a következő lépések alapján megy végbe:

1. A helyi eszköz kihirdeti jelenlétét a virtuális áramkörön a 3. rétegbeli címének kiküldésével.
2. A távoli eszköz fogadja ezt az információt és hozzárendeli a kapott 3. rétegbeli IP-címet a helyi 2. rétegbeli DLCI címéhez.
3. A távoli eszköz is hirdeti saját IP-címét a virtuális áramkörön.
4. A helyi eszköz azon DLCI-hez rendeli a távoli eszköz 3. rétegbeli címét, amelyen keresztül fogadta az információt.

A helyi kezelőfelület (Local Management Interface, LMI) egy jelzési rendszerre vonatkozó szabvány, amit a DTE eszköz és a Frame Relay kapcsoló használ egymás között. Az LMI a kapcsolat kezeléséért és az eszközök közötti állapotok fenntartásáért felelős.

Az LMI üzenetek kommunikációt és szinkronizációt biztosítanak a Frame Relay hálózat és a felhasználó végponti eszköze között. Szabályos időközönként tájékoztatnak az új PVC-k létrejöttéről, a meglévő PVC-k törléséről, továbbá informálnak arról is, hogy a korábban létrehozott PVC-k továbbra is léteznek. A virtuális áramkör állapot-üzenetek megakadályozzák az adatok küldését a már nem létező PVC-k irányába.

Az LMI kapcsolatállapot információt szolgáltat azon virtuális áramkörökől, melyek a Frame Relay leképzési táblázatban (map table) jelennek meg:

Aktív állapot (Active State)

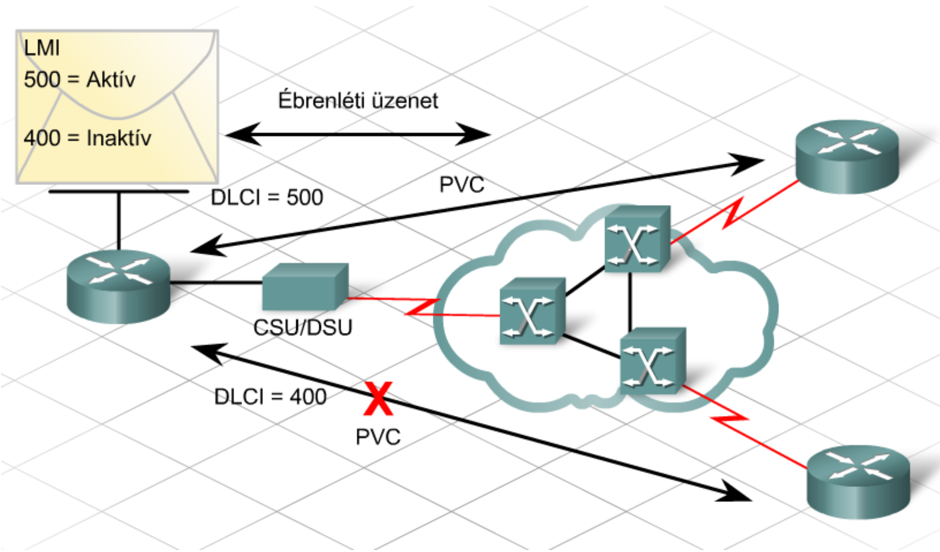
- A kapcsolat aktív, a forgalomirányítók képesek az adatcserére.

Inaktív állapot (Inactive State)

- A helyi végpont és az Frame Relay (FR) kapcsoló közötti összeköttetés működőképes, viszont a FR kapcsoló és a távoli végpont közötti összeköttetés nem megfelelő.

Törölt állapot (Deleted State)

- A helyi kapcsolat nem fogad LMI üzeneteket a FR kapcsolótól, vagy a szolgáltatás nem üzemel a CPE forgalomirányító és a Frame Relay kapcsoló között.



Amikor egy végfelhasználó Frame Relay szolgáltatásra fizet elő, bizonyos szolgáltatási paramétereket egyeztetnie kell a szolgáltatóval.

Az egyik ilyen paraméter a vállalt adatsebesség (Committed Information Rate, CIR). A CIR értéke az a minimális sávszélesség, melyet a szolgáltató az adatok továbbítására garantál a virtuális áramkörön.

A szolgáltató a CIR értékét egy adott egységnyi időtartam alatt átvitt átlagos adatmennyiség alapján számolja ki. A kiszámolt időintervallum értéke a vállalási idő (committed time, Tc). A Tc-n belül vállalt bitek száma a vállalt löket (committed burst, Bc). A Frame Relay szolgáltatás költsége a kapcsolat sebességétől és a CIR értékétől függ.

A CIR ugyan meghatároz egy minimálisan biztosítandó sebességet, azonban ha nincs torlódás az összeköttetéseken, akkor a szolgáltató megnöveli a sávszélességet a második előzetesen elfogadott sávszélesség értékéig.

A túllépési adatsebesség (Excess Information Rate, EIR) a CIR által rögzített érték feletti átlagos sebesség, amelyet a virtuális áramkör akkor biztosít, ha nincs túlterhelve a hálózat. Minden ráadás bit, amely a vállalt adatsebességen túl forgalmazható, egészen a hozzáférési kapcsolat maximális sebességéig, többlet löket (excess Burst, Be) néven ismert.

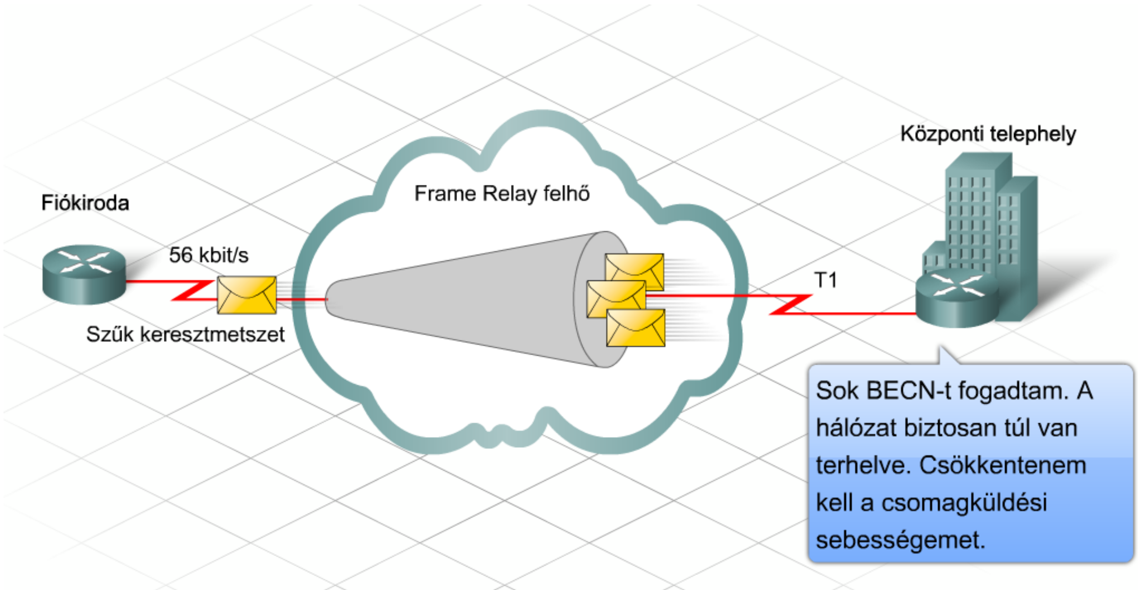
A vállalt adatsebességen (CIR) túli keretek továbbítását nem garantálja a szolgáltatás, de biztosítja, ha a hálózati terhelés lehetővé teszi azt. Az ilyen többlet kereteket figyelmen kívül hagyhatóként (Discard Eligible, DE) jelöli meg a rendszer. Ha torlódás következne be, a szolgáltató először a DE értékkel beállított kereteket dobja el.

A felhasználók gyakran alacsonyabb CIR értékkel rendelkező kapcsolatra fizetnek elő, arra a tényre alapozva, hogy a szolgáltató nagyobb sávszélességet biztosít és meggyorsítja az adatforgalmat, ha nincs torlódás a hálózaton.

Az előremutató explicit torlódásjelzés (Forward Explicit Congestion Notification, FECN) egy egybites mező, melynek értékét 1-re állíthatják a kapcsolók. Ez azt jelzi a végponti DTE eszközök számára, hogy torlódás lépett fel a hálózatban a célhálózat felé vezető irányban.

A visszirányú explicit torlódásjelzés (Backward Explicit Congestion Notification, BECN) egy egybites érték, melyet a Frame Relay kapcsolók akkor állítanak 1-es értékűre, ha a hálózaton torlódás lép fel az ellenkező, azaz a forráshálózat irányában.

A FECN és BECN bitek segítségével a magasabb szintű protokollok intelligensen reagálhatnak ezekre a torlódásjelzésekre. A küldő eszköz például a BECN-t figyelembe véve lassíthatja az átviteli sebességét.



7.4 A fejezet összefoglalása

- Egy WAN számos különböző technológiát használ, mindegyik más-más előnyökkel rendelkezik.
- A használatban lévő technológia függvényében, az adatok elfogadható formátumúvá átalakításához egy modemre vagy egy CSU/DSU-ra van szükség.
- A WAN technológiák feloszthatóak vonalkapcsolt, csomagkapcsolt és cellakapcsolt (53 bájtos csomag a cella) típusúakra.
- A vonalkapcsolt technológiák egy fizikai áramkört hoznak létre a végberendezések között, mielőtt információkat küldenének.
- A csomag- és cellakapcsolt technológiák PVC vagy SVC áramköröket használnak az információküldéshez a hálózaton keresztül (kivéve a DG típusúakat).
- A WAN technológiák lehetnek "last mile" típusúak, amelyek a szolgáltatókat kötik össze az ügyfelekkel, illetve lehetnek nagy távolságúak, melyek a szolgáltatókat kötik össze egymással.
-
- A HDLC az alapértelmezett 2. rétegbeli, soros vonali beágyazási típus a Cisco forgalomirányítókon.
- A Cisco HDLC bevezet egy külön adatmezőt, hogy lehetővé tegye többféle 3. rétegbeli protokoll hordozását.
- A 2. rétegbeli beágyazási típus megváltozik, miközben a keretek a WAN hálózaton keresztül haladnak át.
- A PPP lehetővé teszi számos fejlett szolgáltatás egyeztetését, mint például hitelesítés, terheléselosztás, visszahívás és tömörítés.
- A PPP támogatja a PAP és a CHAP hitelesítést is.
- A PAP hitelesítés nyílt szöveges formátumban küldi el a felhasználói név/jelszó párost és ki van téve a lehallgatásos és a visszajátszásos támadásoknak.
- A CHAP beállítható időközönként kihívásokat bocsát ki és újra-hitelesítésre kényszeríti a csatlakoztatott eszközt.
- A Frame Relay egy csomagkapcsolt technológia.
- A Frame Relay virtuális áramköröket használ egy adott forrás célállomáshoz való csatlakoztatásához. A virtuális áramkörök lehetnek kapcsoltak vagy állandóak.
- A Frame Relay FECN és BECN bitek segítségével tájékoztatja a fogadó és a küldő eszközöket a hálózati torlódásról, így a forgalomirányítók elvégezhetik a szükséges műveleteket.
- A Frame Relay olyan paramétereket használ, mint a CIR, hogy megállapítsa az egyes virtuális áramkörökön használható sávszélesség mértékét.

8. Forgalomszűrés hozzáférési listák használatával

8.1 A hozzáférési listák használata

8.1.1 Forgalomszűrés

A vállalati hálózaton belül a biztonság alapvető fontosságú. Fontos az illetéktelen felhasználók belépésének megakadályozása és a hálózat védelme a különféle támadásokkal (pl.: DoS támadás) szemben. Az illetéktelen felhasználók módosíthatják, megsemmisíthetik vagy eltulajdoníthatják a kiszolgálókon tárolt fontos adatokat, a DoS támadások pedig megakadályozhatják a jogos felhasználók hozzáférését az erőforrásokhoz. Mindkét eset idő- és pénzveszteséggel jár a vállalat számára.

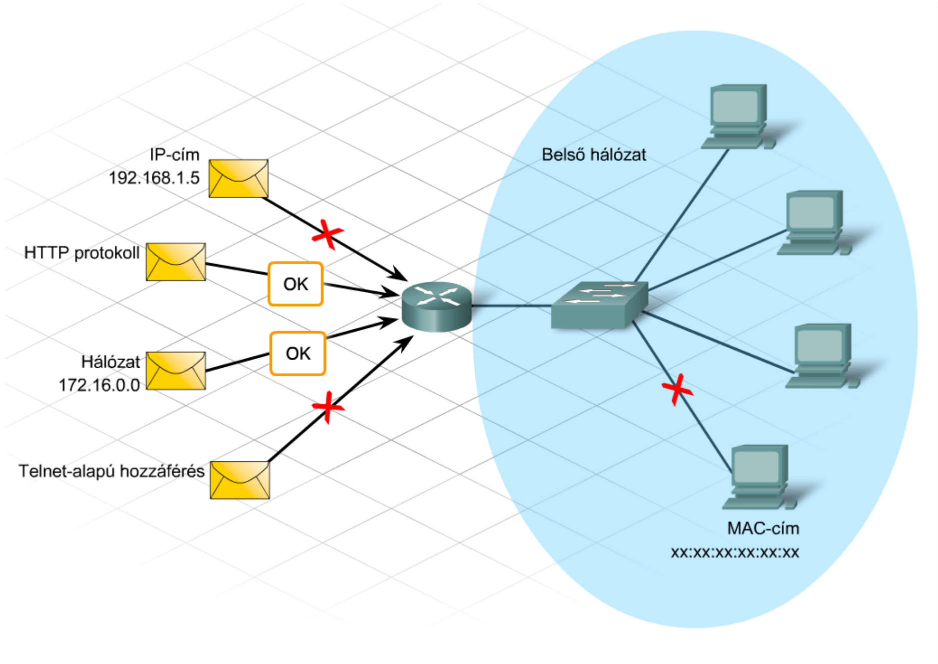
A forgalomszűrés segítségével a hálózati rendszergazda felügyelheti a hálózat különböző részeit. A szűrés a csomagtartalom elemzésének folyamata, amely alapján eldönthető, hogy egy adott csomagot átengedünk vagy blokkolunk.

A csomagszűrés lehet egyszerű vagy összetett, a forgalom engedélyezése vagy tiltása az alábbiak szerint történhet:

- Forrás IP-cím
- Cél IP-cím
- MAC-cím
- Protokollok
- Alkalmazástípus

A csomagszűrés a levélszemét szűréséhez hasonlítható. A legtöbb levelezőprogramban a felhasználó beállíthatja, hogy egy bizonyos forráscímről érkező levelek automatikusan törlődjenek. A csomagszűrés ugyanígy végezhető: be kell állítani a forgalomirányítót a nemkívánatos forgalom azonosítására.

A forgalomszűrés javítja a hálózat teljesítményét. A nemkívánatos forgalom forráshoz közeli tiltásával a forgalom nem halad keresztül a hálózaton, és nem pazarol el értékes erőforrásokat.



A forgalomszűréshez használt leggyakoribb eszközök:

- Integrált forgalomirányítóba épített tűzfalak
- Adatbiztonsági funkciókat ellátó célkészülékek
- Kiszolgálók

Az eszközök némelyike kizárólag a belső hálózatból származó forgalmat szűri. A jóval kifinomultabb biztonsági eszközök felismerik és kiszűrik a külső forrásból érkező ismert támadástípusokat.

A vállalati forgalomirányítók felismerik a kártékony forgalmat, és megakadályozzák, hogy az bejusson a hálózatba és ott kárt okozzon. Szinte minden forgalomirányító képes a forrás és cél IP-cím alapján történő csomagszűrésre, emellett meghatározott alkalmazások és protokollok (pl. IP, TCP, HTTP, FTP és Telnet) szerinti szűrésre is alkalmasak.



8.1.2 A hozzáférés-vezérlési listák

A forgalomszűrés egyik legáltalánosabb módja a hozzáférés-vezérlési listák (Access Control List, ACL) használata. Az ACL-ek használatával a hálózatba belépő és az onnan távozó forgalom ellenőrizhető és szűrhető.

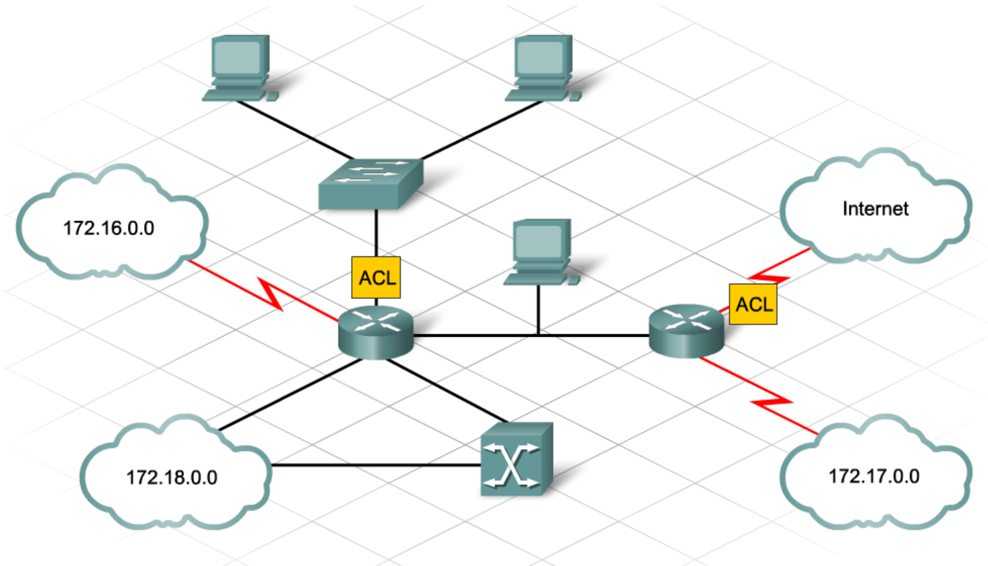
Méretét tekintve az ACL lehet egy adott forrásból érkező forgalmat engedélyező vagy tiltó egyetlen parancs, de lehet több száz parancsból álló lista is, ami különböző forrásból érkező csomagok átengedéséről vagy tiltásáról dönt. Az ACL elsődlegesen az engedélyezni vagy elutasítani kívánt csomagtípusok azonosítására használható.

Az ACL által azonosított forgalom az alábbi célokra is felhasználható:

- A belső állomások meghatározása címfordításhoz
- A speciális funkciókhoz (pl. a szolgáltatásminőség /QoS - Quality of Service/, sorba állítás) tartozó forgalom azonosítása és csoportosítása
- A forgalomirányítási frissítések tartalmi korlátozása
- A hibakeresési üzenetek korlátozása
- A forgalomirányítók virtuális terminálról történő elérésének szabályozása

Az ACL-ek használatából eredő potenciális problémák:

- Az összes csomag ellenőrzése komoly terhelést jelent a forgalomirányító számára, így kevesebb idő jut a csomagtovábbításra.
- A rosszul megtervezett ACL-ek még nagyobb terhelést okoznak, ami zavart okozhat a hálózat használatában.
- A nem megfelelően elhelyezett ACL-ek blokkolhatják az engedélyezni kívánt, és engedélyezhetik a blokkolni kívánt forgalmat.



8.1.3 Az ACL típusok és használatuk

A hozzáférési listák létrehozásakor a hálózati rendszergazda számos lehetőség közül választhat, a szükséges ACL típusát mindig a tervezési irányelvek összetettsége határozza meg.

Három ACL típus létezik:

Normál ACL

A normál ACL (Standard ACL) a legegyszerűbb a három típusból. Normál IP ACL létrehozásakor az ACL a csomag forrás IP-címének alapján végzi a szűrést. A normál ACL a teljes (pl. IP) protokollműködés alapján engedélyezi vagy tiltja a forgalmat. Ha például egy normál ACL nem engedélyezi egy hálózati állomás IP forgalmát, akkor az állomásról érkező összes szolgáltatást tiltja. Ez az ACL-típus egy adott felhasználó vagy LAN számára engedélyezheti az összes szolgáltatás elérését a forgalomirányítón keresztül, míg az összes többi IP-cím esetén tiltja a hozzáférést. A normál ACL-ek a hozzájuk rendelt azonositási szám alapján azonosíthatók. Az IP-forgalom engedélyezését vagy tiltását végző hozzáférési listák azonosítási száma 1 és 99, illetve 1300 és 1999 közötti lehet.

Kiterjesztett ACL

A kiterjesztett ACL (Extended ACL) nem csupán a forrás IP-cím, hanem a cél IP-cím, a protokoll és a portszámok alapján is szűrhet. A kiterjesztett ACL-ek használata sokkal elterjedtebb, mint a normál ACL-eké, mivel specifikusabbak és jobb ellenőrzést tesznek lehetővé. A kiterjesztett ACL-ek azonositási száma 100 és 199, illetve 2000 és 2699 közötti lehet.

Nevesített ACL

A nevesített ACL (Named ACL, NACL) olyan normál vagy kiterjesztett hozzáférési lista, amelyre szám helyett egy beszédes névvel hivatkozunk. A nevesített ACL-ek beállítása a forgalomirányító NACL üzemmódjában történik.

Az IOS hozzáférési listák típusai

ACL típus	ACL parancs/utasítás	Utasítás célja
Normál	Router(config)#**access-list 1 permit host 172.16.2.88**	• Egy bizonyos IP-címet engedélyez.
Kiterjesztett	Router(config)#**access-list 100 deny tcp 172.16.2.0 0.0.0.255 any eq telnet**	• Tiltja a 172.16.2.0/24 alhálózat számára bármely más állomás elérését, amennyiben telnetkapcsolatot próbálnak létesíteni.
Nevesített	Router(config)#**ip access-list standard permit-ip** Router(config-ext-nacl)#**permit host 192.168.5.47**	• Létrehoz egy permit-ip nevű normál hozzáférési listát. • Engedélyezi a hozzáférést a 192.168.5.47 IP-címről. • Az első parancs a forgalomirányítót NACL konfigurációs almódba helyezi.

7.1.4 Az ACL feldolgozása

A hozzáférési listák egy vagy több utasításból állnak. A forgalmat minden egyes utasítás a megadott paraméterek alapján engedélyezheti vagy tilthatja. Az ACL-ben található utasításokat sorban egymás után össze kell vetni a forgalommal, egészen addig, amíg paraméter egyezést nem találunk vagy el nem érjük az utasításlista végét.

Az ACL utolsó utasítása mindig implicit tiltás. Ez az utasítás automatikusan is odakerül mindegyik ACL végére, még akkor is, ha a konfigáció készitője nem irja oda. Az implicit tiltás semmilyen forgalmat nem engedélyez. Ezért az implicit tiltás funkció megakadályozza a nemkívánatos forgalom véletlen áthaladását.

A hozzáférési lista akkor lép működésbe, ha elkészítése után hozzárendeljük a megfelelő interfészhez. Az ACL az interfészen, a beállítástól függően, vagy a bejövő vagy a kimenő forgalmat figyeli. Amennyiben az ACL egy engedélyező utasításának előírása megegyezik az éppen vizsgált csomag paramétereivel, a csomag továbbhaladása engedélyezett. Ha a csomaghoz egy tiltó utasítás illeszkedik, akkor nem haladhat tovább. Az engedélyező utasítást nem tartalmazó ACL minden forgalmat tilt, mivel minden ACL végén szerepel az implicit tiltás. Az ACL tehát minden olyan forgalmat tilt, ami nincs konkrétan engedélyezve.

A rendszergazda akár befelé akár kifelé irányuló forgalmat szűrő ACL listát rendelhet a forgalomirányító bármely interfészéhez. A bejövő vagy kimenő irányt mindig a forgalomirányító szemszögéből nézzük, így az interfészre beérkező forgalom bejövő (a forgalomirányitóba belépő), az onnan távozó forgalom pedig kimenő.

Amikor egy csomag érkezik valamely interfészre, a forgalomirányító az alábbi paramétereket ellenőrzi:

- Létezik-e az interfészhez rendelt ACL lista?
- Az ACL lista a bejövő vagy a kimenő forgalomra vonatkozik?
- A forgalomra teljesül-e valamely engedélyező vagy tiltó feltétel?

Az interfész kimenő irányához hozzárendelt ACL semmilyen hatással nincs az adott interfész beérkező forgalmára, ami fordítva is igaz.

A forgalomirányító interfészekhez protokollonként és irányonként egy-egy ACL adható meg. Igy az IP protokoll esetében is egy interfészhez egyszerre csak egy befelé és egy kifelé haladó forgalmat szűrő ACL adható meg.

Az interfészhez hozzárendelt ACL-ek végrehajtása késlelteti a forgalmat. Akár egyetlen hosszú ACL is észrevehető hatással lehet a forgalomirányító teljesítményére.

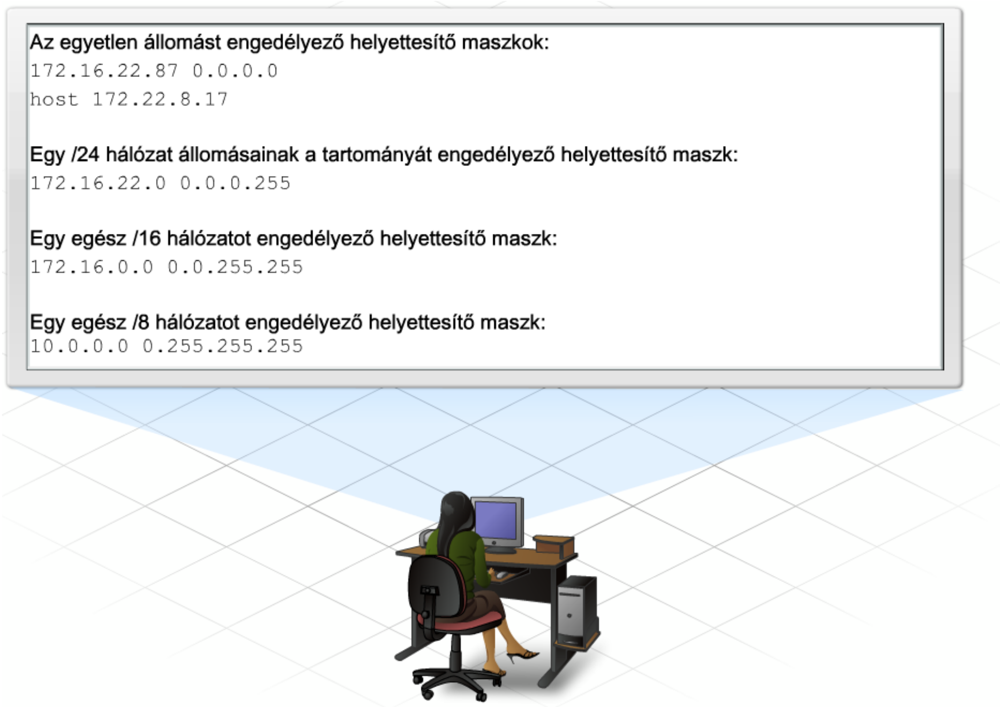
8.2 A helyettesítő maszk használata

8.2.1 A helyettesítő maszk célja és felépítése

Alapesetben az egyszerű ACL-ek csak egyetlen címet engedélyeznek vagy tiltanak. Több cím vagy egy adott címtartomány szűréséhez több utasítás vagy megfelelő helyettesítő maszk szükséges. Az IP-cím és a helyettesítő maszk együttes használata sokkal rugalmasabb megoldást nyújt. A helyettesítő maszk lehetővé teszi egy adott címtartomány, vagy akár egy egész hálózat szűrését egyetlen utasítás segítségével.

A helyettesítő maszkban a 0-k jelölik ki az IP-cím azon bitjeit, amiknek pontosan egyeznie kell a megadott címmel, míg a 1-eseknél nincs szükség egyezésre.

A 0.0.0.0 helyettesítő maszk pontos egyezést ír elő az IP-cím mind a 32 bitjén. Ez a maszk egyenértékű a host paraméterrel



Az ACL-ek által használt helyettesítő maszk hasonlít az OSPF irányítóprotokoll esetében használt maszkhoz. Ennek ellenére a két maszk eltérő célra szolgál. Az ACL-utasításokban szereplő helyettesítő maszk az engedélyezni vagy tiltani kívánt címtartományt határozza meg.

Egy ACL-utasításban az IP-cím és a hozzá tartozó helyettesítő maszk közösen, együttesen határozzák meg, hogy az utasítás mely címbitjeit kell összehasonlítani a vizsgált csomagok megfelelő cimbitjeivel. Az interfészre beérkező vagy onnan távozó összes csomag címrészét össze kell hasonlítani az ACL-utasítások megfelelő címrészével, hogy van-e egyezés. A helyettesítő maszk határozza meg, hogy összehasonlításkor a csomag fejlécében szereplő IP-cím és az utasításban megadott cím mely bitjeit kell figyelembe venni.

Az alábbi utasítás például a 192.168.1.0 hálózat minden állomását engedélyezi, ugyanakkor minden mást tilt:

```
access-list 1 permit 192.168.1.0 0.0.0.255
```

A helyettesítő maszk meghatározza, hogy csupán az első három oktettnek kell illeszkednie. A fentiekből következik, hogy ha a bejövő csomag első 24 bitje megegyezik a viszonyítási mező első 24 bitjével, akkor a csomag engedélyezve lesz. A helyettesítő maszk szerint bármely csomag, amelynek forrás IP-címe a 192.168.1.1 és a 192.168.1.255 közötti tartományba esik, illeszkedni fog a példában szereplő összehasonlítási címhez. Minden más csomagot az ACL implicit tiltás (deny any) utasítása letilt.

```
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

	Decimális megfelelő	Bináris megfelelő
Összehasonlítási cím:	192.168.1.0	11000000.10101000.00000001.00000000
Helyettesítő maszk:	0.0.0.255	00000000.00000000.00000000.11111111
Az összehasonlítási cím illeszkedéshez szükséges bitjei:	192.168.1.X	11000000.10101000.00000001.XXXXXXXX
Bejövő csomag címe:	192.168.1.27	11000000.10101000.00000001.00011011

8.2.2 A helyettesítő maszk hatásainak elemzése

Egy ACL létrehozásakor két speciális helyettesítő maszk egyszerűbb alakban is megadható: a host (állomás) és az any (bármi).

A host paraméter

Egy bizonyos állomás szűréséhez az IP-cím utáni 0.0.0.0 helyettesítési maszkot, vagy az IP-cím előtti host paramétert kell használnunk.

```
R1(config)#access-list 9 deny 192.168.15.99 0.0.0.0
```

Ugyanaz, mint:

```
R1(config)#access-list 9 deny host 192.168.15.99
```

Az any paraméter

Az összes állomás szűréséhez használjuk a csupa egyesekből álló paramétert, amelyet a 255.255.255.255 helyettesítő maszk beállításával adhatunk meg! A 255.255.255.255 helyettesítő maszk az összes bitet egyezőnek tekinti, ezért általában az IP-címet a 0.0.0.0 jelöli. Az összes állomás szűrésére használt másik módszer az any paraméter használata.

```
R1(config)#access-list 9 permit 0.0.0.0 255.255.255.255
```

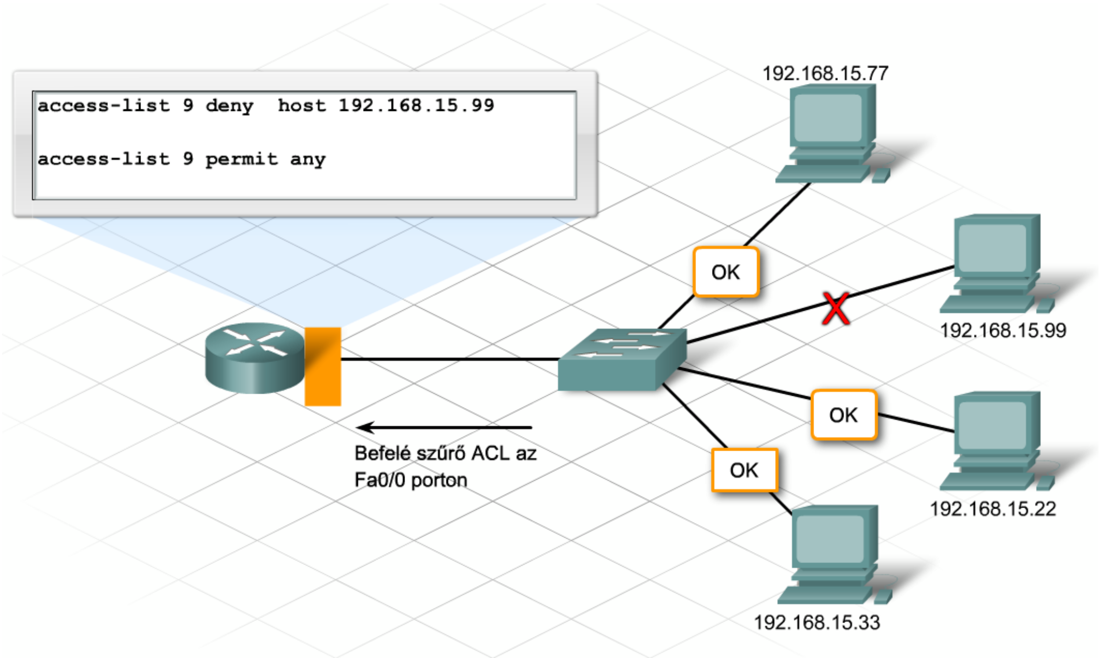
Ugyanaz, mint:

```
R1(config)#access-list 9 permit any
```

Nézzük meg az alábbi példát, amely egy bizonyos állomást letilt, míg az összes többit engedélyezi:

```
R1(config)#access-list 9 deny host 192.168.15.99
R1(config)#access-list 9 permit any
```

A permit any parancs minden forgalmat engedélyez, amely az ACL-ben nincs konkrétan elutasítva. Ezzel a beállítással egyik csomag sem éri el az ACL végén szereplő implicit deny any utasítást.



A többszintű IP-címzési sémát használó vállalati hálózatokban gyakran szükséges az alhálózati forgalom szűrése.

Amennyiben a 192.168.77.0 hálózat alhálózatokra osztásához 3 bitet használunk, az alhálózati maszk 255.255.255.224 lesz. Ha a fenti alhálózati maszkot kivonjuk a csupa 255-ből álló 32 bites hálózati maszkból, a 0.0.0.31 helyettesítő maszkot kapjuk. Ennek megfelelően a 192.168.77.32 alhálózat állomásainak engedélyezéséhez az alábbi ACL utasítást kell használnunk:

```
access-list 44 permit 192.168.77.32 0.0.0.31
```

Minden csomag első 27 bitje megegyezik a viszonyítási cím első 27 bitjével. A fenti utasítás által engedélyezett teljes címtartomány a 192.168.77.33-tól a 192.168.77.63-ig terjed, amely pontosan lefedi a 192.168.77.32 alhálózat összes címét.

Alhálózati cím: 192.168.77.32 255.255.255.224

Bitérték	128	64	32	16	8	4	2	1	Decimális érték
csupa 1-es	1	1	1	1	1	1	1	1	255
Alhálózati maszk	1	1	1	0	0	0	0	0	224
Helyettesítő maszk	0	0	0	1	1	1	1	1	31

Illeszkedő bitek — Nem illeszkedő bitek

Összehasonlítási/kiindulási cím: 192.168.77.32 0.0.0.31

A teljes A, B vagy C osztályú hálózatok alhálózati és helyettesítő maszkja egyenlően oszlik meg egy oktetthatáron. A nem oktetthatárra eső alhálózatok eltérő helyettesítő maszkot eredményeznek. Az oktetthatár az első és második, vagy a második és harmadik oktett közé eső rész.

Példa: Egy alapértelmezés szerinti A osztályú alhálózat esetében a 8. és 9. bit közé esik. Ez az egyik oktett vége és a következő oktett eleje, amit a következő oktett határának nevezünk.

A forgalom finomhangolásához szükséges vezérlést az ACL utasításokhoz létrehozott helyettesítő maszkok biztosítják. Kezdők számára a különböző alhálózatok forgalmának szűrését a legnehezebb megérteni.

A 192.168.77.0 hálózat a 255.255.255.192 vagy a /26 alhálózati maszkkal az alábbi négy alhálózatot jelenti:

192.168.77.0/26

192.168.77.64/26

192.168.77.128/26

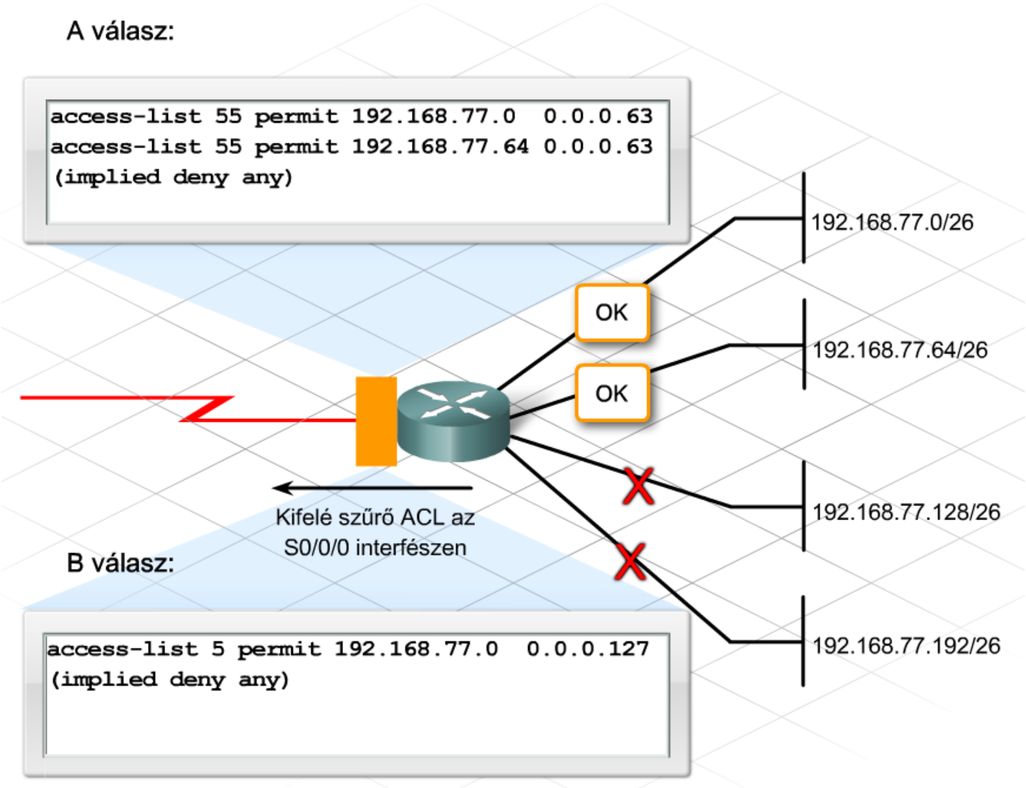
192.168.77.192/26

A fenti négy alhálózat bármelyikét szűrő ACL létrehozásához vonjuk ki a 255.255.255.192 alhálózati maszkot a csupa 255-ből álló maszkból, amely a 0.0.0.63 helyettesítő maszkot eredményezi. Az első két alhálózatból érkező forgalom engedélyezéséhez két ACL utasítást kell használnunk:

```
access-list 55 permit 192.168.77.0 0.0.0.63
access-list 55 permit 192.168.77.64 0.0.0.63
```

Az első két alhálózat összevonható a 192.168.77.0/25 megadásával. A 255.255.255.128 összevont alhálózati maszk kivonása a csupa 255-ből álló maszkból a 0.0.0.127 helyettesítő maszkot eredményezi. A fenti maszk használatával a két alhálózat kettő helyett egyetlen ACL-ben összefogható.

```
access-list 5 permit 192.168.77.0 0.0.0.127
```



8.3 A hozzáférési listák paraméterezése

8.3.1 A normál és a kiterjesztett ACL-ek elhelyezése

A megfelelően megtervezett hozzáférési listák pozitív hatással vannak a hálózati teljesítményre és rendelkezésre állásra. Tervezzünk meg a hozzáférési listák létrehozását és elhelyezését a maximális hatás érdekében!

A tervezés az alábbi lépésekből áll:

1. A forgalomszűrési igények meghatározása.
2. Az igényeknek leginkább megfelelő ACL típusának kiválasztása.
3. Annak a forgalomirányítónak és interfésznek a kiválasztása, amelyhez az ACL-t rendeljük.
4. A forgalomszűrés irányának meghatározása

1 lépés: A forgalomszűrési igények meghatározása

Gyűjtsük össze a forgalomszűrési igényeket az érintettektől, a vállalat minden osztályáról! A fenti – felhasználói igényeken, forgalomtípuson, terheltségen és biztonsági szempontokon alapuló –igények vállalatonként eltérőek lehetnek.

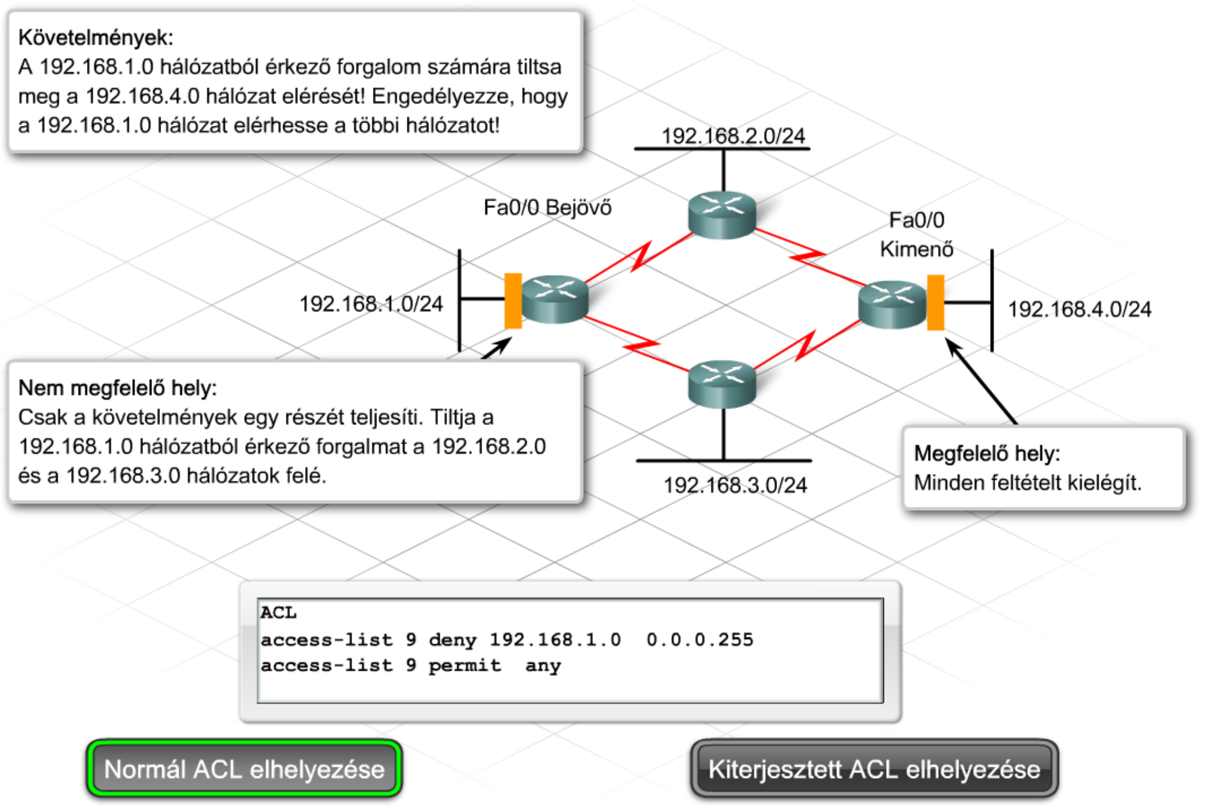
2. lépés: Az igényeknek leginkább megfelelő ACL típusának kiválasztása

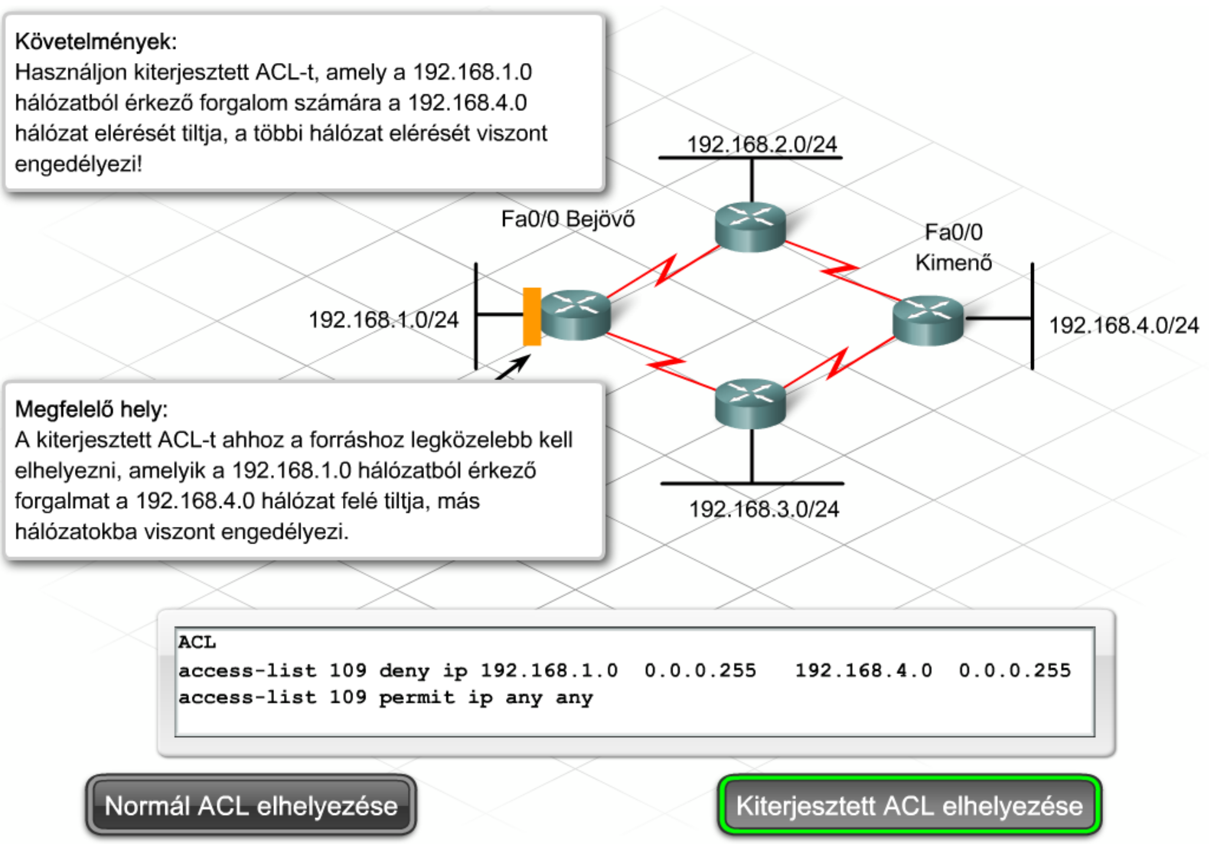
Mindig a helyzetnek megfelelő szűrési igényeken múlik, hogy normál vagy kiterjesztett ACL-t használunk. Az ACL típusának kiválasztása hatással lehet az ACL rugalmasságára csakúgy, mint a forgalomirányító teljesítményére és a hálózati kapcsolat sávszélességére.

A normál ACL létrehozása és alkalmazása egyszerű. A normál ACL viszont kizárólag a forráscím alapján képes szűrni, tekintet nélkül a forgalom típusára és céljára. A több hálózatba vezető útvonalak esetében egy, a forráshoz túl közel elhelyezett ACL akaratlanul is letilthatja az engedélyezni kívánt forgalmat is. Ezért fontos, hogy a normál ACL-eket a célhoz a lehető legközelebb helyezzük el!

Ha a szűrési igények jóval összetettebbek, használjunk kiterjesztett ACL-t! A kiterjesztett ACL precizebb szelekciót biztosít, mint a normál ACL. Forrás- és célcím szerinti szűrésre egyaránt képes. Szükség esetén a hálózati és szállítási réteg protokolljai és a portszámok alapján is szűrhet. Ez a megnövelt szűrési részletesség lehetővé teszi a hálózati rendszergazda számára a biztonsági terv igényeinek megfelelő ACL-ek létrehozását.

A kiterjesztett ACL-t mindig a forráscímhez közel helyezzük el! Ha az ACL mind a forrás-, mind a célcímet megvizsgálja, akkor bizonyos célhálózatba szánt csomagokat még azelőtt letilthat, hogy azok elhagynák a forrás-forgalomirányítót. A csomagok szűrése még a hálózaton történő áthaladásuk előtt történik, ami segít a sávszélesség megőrzésében.





3. lépés: A megfelelő forgalomirányító és interfész meghatározása, amelyhez az ACL-t rendeljük

Helyezzük az ACL-eket a hozzáférési vagy az elosztási réteg forgalomirányítóira! A hálózati rendszergazdának megfelelő jogosultságokkal kell rendelkeznie a fenti forgalomirányítók

vezérléséhez és a biztonsági irányelvek alkalmazásához. Az a hálózati rendszergazda, aki nem rendelkezik hozzáféréssel a forgalomirányítóhoz, az ACL-t sem képes ott beállítani.

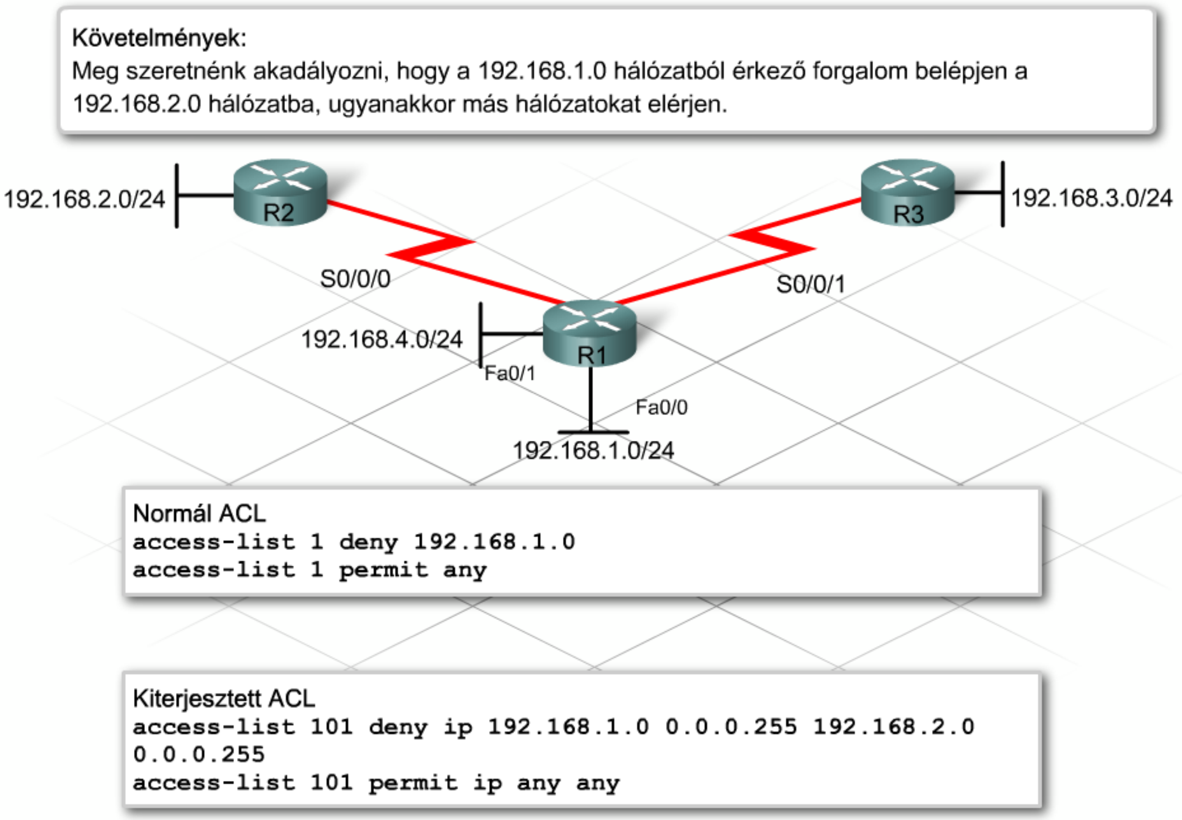
A megfelelő interfész kiválasztásához a szűrési igényeket, az ACL típusát és a forgalomirányító hálózaton belüli pozícióját egyaránt figyelembe kell venni. A forgalom szűrését még azelőtt célszerű elvégezni, hogy az elérne egy alacsonyabb sávszélességű soros összeköttetést. Az interfész kiválasztása a forgalomirányító kijelölését követően már általában egyértelmű.

4. lépés: A forgalomszűrés irányának meghatározása

Szemléljük a forgalom áramlását a forgalomirányító szemszögéből azért, hogy az ACL alkalmazásának irányát meg tudjuk határozni!

Bejövő forgalom a forgalomirányító valamely interfészére kívülről érkező forgalom. A forgalomirányító összeveti a beérkező csomagot az ACL-lel, mielőtt megkeresné a célhálózatot az irányítótáblában. Az itt elutasított csomagok megspórolják az irányítótáblában történő keresés költségét. Emiatt a befelé szűrő hozzáférési lista jóval hatékonyabb a forgalomirányító számára, mint a kifelé szűrő hozzáférési lista.

A kimenő forgalom a forgalomirányítón belül áramlik, majd onnan valamelyik interfészen keresztül távozik. A kimenő csomagra vonatkozóan a forgalomirányító már elvégezte az irányítási keresést, és a csomagot a megfelelő interfészre kapcsolta. A csomag összevetése az ACL-lel közvetlenül a forgalomirányítóról való távozás előtt történik.



8.3.2 Az ACL alapbeállításának folyamata

Az igények összegyűjtése, a hozzáférési lista megtervezése és az alkalmazási hely meghatározása után el kell készíteni az ACL-t.

Mindegyik ACL egyedi azonosítót igényel, amely lehet egy szám vagy egy beszédes név.

A számozott hozzáférési listákban a szám meghatározza a létrehozott ACL típusát:

- A normál IP ACL-ek azonosító száma 1 és 99 között, illetve 1300 és 1999 között lehet.
- A kiterjesztett IP ACL-ek azonosító száma 100 és 199 között, valamint 2000 és 2699 között mozoghat.

AppleTalk és IPX ACL létrehozása szintén lehetséges.

Egy forgalomirányító bármely interfészére protokollonként és irányonként legfeljebb egy ACL-t lehet hozzárendelni. Amennyiben a forgalomirányító kizárólag IP-t futtat, mindegyik interfész legfeljebb két ACL-t kezelhet: egy befelé és egy kifelé szűrőt. Mivel minden, az adott interfészen áthaladó csomagot össze kell vetni mindegyik ACL-lel, ezért az ACL késleltetést okoz.

ACL feldolgozási és létrehozási irányelvek

- Irányonként és protokollonként csak egy ACL adható meg.
- A normál ACL-eket a célhoz a lehető legközelebb kell elhelyezni.
- A kiterjesztett ACL-eket a forráshoz a lehető legközelebb kell elhelyezni.
- Mindig a lista típusának megfelelő számtartományt kell használni.
- A bejövő vagy kimenő irány meghatározásához az interfészt mindig a forgalomirányító szemszögéből kell nézni.
- Az utasítások feldolgozása egymás után, felülről lefelé haladva történik.
- Amennyiben egy csomagra nincs illeszkedés, eldobásra kerül.
- A hozzáférési lista utasításait mindig a konkréttól az általános felé haladva kell megadni.
- Az ACL-ben mindig szerepeljen egy **permit** utasítás, máskülönben minden forgalom tiltásra kerül.

További információ

- Az IP alapú hozzáférési listák a célállomás elérhetetlenségét jelző ICMP-üzenetet küldenek az elutasított csomagok forrásainak, majd eldobják a csomagokat.
- A kimenő szűrők nem vonatkoznak a helyi forgalomirányítóról kiinduló forgalomra.
- Minden hozzáférési lista végén egy (a listában nem szereplő) implicit **deny any** utasítás található.
- A könnyebb szerkeszthetőség érdekében érdemes az ACL-eket egy szövegszerkesztőben létrehozni. Így az ACL utasításokat kimásolhatjuk és beilleszthetjük a

Egy hozzáférési lista konfigurálása két lépésből áll: létrehozás és alkalmazás.

Az ACL létrehozása

Lépjünk be a globális konfigurációs módba! Az access-list parancs használatával adjuk meg a hozzáférési lista utasításait! Az összes utasítást ugyanazzal az ACL számmal lássuk el, amíg a hozzáférési lista nem lesz teljes!

A normál ACL utasítás-szintaktikája az alábbi:

```
access-list [hozzáférési_lista_száma] [deny|permit] [forráscím]
[forrás_helyettesítő_maszk][log]
```

Mindaddig, amíg nincs egyezés, minden csomagot össze kell vetni az összes ACL utasítással, ezért az utasítások ACL-en belüli sorrendje nagymértékben befolyásolhatja a már említett késleltetést. A fentiek miatt, az utasítások sorrendjénél érdemes a gyakoribb feltételeket a kevésbé gyakoriak elé helyezni! A forgalom döntő részét képező utasításokat például tegyük mindig az ACL elejére!

Azt azonban tartsuk fejben, hogy egyezés esetén a csomag már nem lesz összevetve az ACL további utasításaival! Ez azt jelenti, hogy ha az egyik sor engedélyez egy csomagot, de az ACL egy későbbi sora tiltja azt, a csomag engedélyezve lesz. Ezért úgy tervezzük meg az ACL-t, hogy a konkrétabb feltételek az általánosabbak előtt szerepeljenek! Másképpen fogalmazva, először tiltsuk le egy hálózat bizonyos állomását, és csak azután engedélyezzük a teljes hálózat maradék részét!

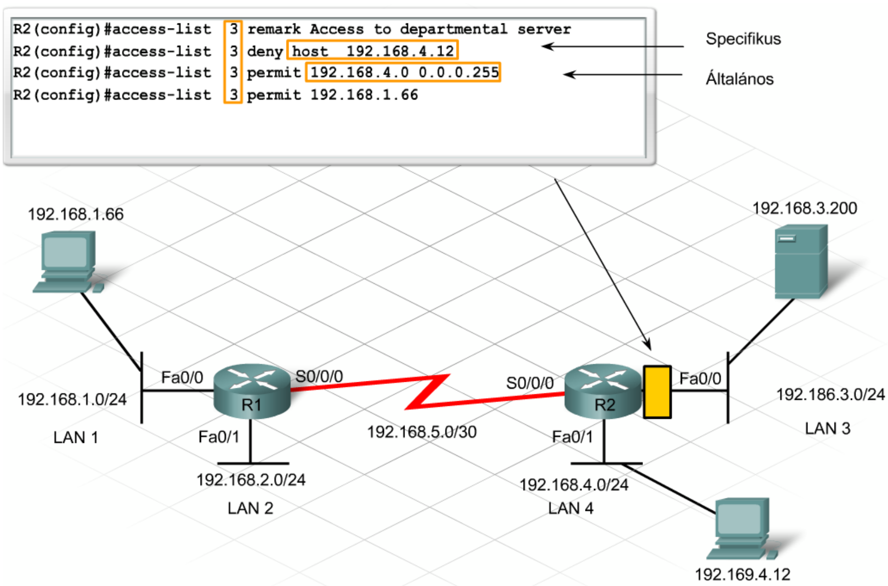
Dokumentáljuk az ACL minden részének vagy utasításának a funkcióját a remark parancs segítségével:

```
access-list [a lista száma] remark [szöveg]
```

Egy ACL törléséhez használjuk az alábbi parancsot:

```
no access-list [a lista száma]
```

Nincs lehetőség arra, hogy csupán a normál vagy kiterjesztett ACL egyetlen sorát töröljük! Ehelyett az egész ACL-t törölni kell, majd a javított listával kell lecserélni.



8.3.3 A számozott normál ACL beállítása

Az ACL addig nem szűri a forgalmat, amíg egy interfészre nem alkalmazzuk, azaz hozzá nem rendeljük az interfészhez.

Az ACL alkalmazása

Rendeljük az ACL-t egy vagy több interfészhez és határozzuk meg, hogy bejövő vagy kimenő forgalomra vonatkozik-e! Az ACL-t a célhoz lehető legközelebb alkalmazzuk!

```
R2(config-if)#ip access-group hozzáférési lista száma [in | out]
```

Az alábbi parancsokkal az 5-ös számú hozzáférési lista az R2 forgalomirányító Fa0/0 interfészére helyezhető, hogy a bejövő forgalmat szűrje:

```
R2(config)#interface fastethernet 0/0
R2(config-if)#ip access-group 5 in
```

Egy interfészre alkalmazott ACL esetében (bizonyos IOS változatok alkalmazásakor) a **kimenő** irány az alapértelmezett, ennek ellenére az irány megadása – a zavarok elkerülése és a forgalom megfelelő irányba történő szűrésének biztosítása érdekében – nagyon fontos.

Az ACL eltávolítása az interfészről az ACL érintetlenül hagyásával, a `no ip access-group interface` paranccsal lehetséges.

```
R2(config)#access-list 3 remark Access to departmental server
R2(config)#access-list 3 deny  host 192.168.4.12
R2(config)#access-list 3 permit 192.168.4.0 0.0.0.255
R2(config)#access-list 3 permit host 192.168.1.66

R2(config)#interface fa0/0
R2(config-if)#ip access-group 3 out
```

Számos ACL paranccsal ellenőrizhető a megfelelő szintaktika, az utasítások sorrendje és az interfészeken történő elhelyezés.

```
show ip interface
```

- A fenti parancs megjeleníti az IP interfész információit, és jelzi a hozzárendelt ACL-eket.

```
show access-lists [hozzáférési lista száma]
```

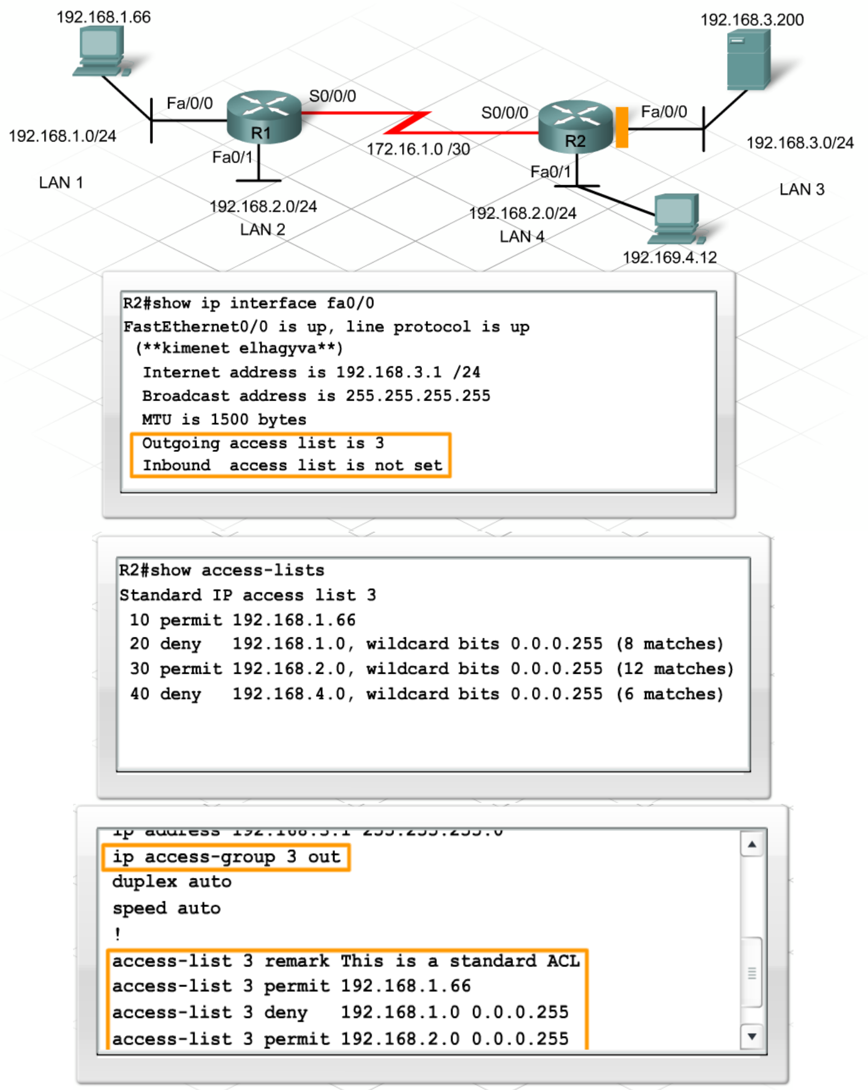
- A fenti parancs nem csupán a forgalomirányító összes ACL-jének tartalmát jeleníti meg, hanem az egyes engedélyező és tiltó utasításokhoz tartozó – az ACL alkalmazása óta talált – egyezések számát is. Egy adott lista megtekintéséhez adjuk meg az ACL nevét vagy számát a parancs paramétereként!

```
show running-config
```

- A fenti parancs megjeleníti a forgalomirányítón beállított összes ACL-t, akkor is, ha azok jelenleg egyik interfészhez sincsenek hozzárendelve.

Számozott ACL használatakor az ACL első létrehozása után hozzáadott parancsok a lista végére kerülnek. Ez a sorrend nem biztos, hogy a kívánt eredményhez vezet. A probléma megoldásához távolítsuk el az eredeti ACL-t, majd a szükséges korrekcióval hozzuk létre ismét!

Jól bevált módszer, ha az ACL-t egy szövegszerkesztőben hozzuk létre, amely lehetővé teszi az ACL könnyű szerkesztését és a forgalomirányító konfigurációjába történő beillesztését. Ugyanakkor arra is figyeljünk oda, hogy az ACL másolása és beillesztése előtt távolítsuk el a jelenleg alkalmazott ACL-t, máskülönben az összes utasítás annak a végére kerül.



8.3.4 A számozott kiterjesztett ACL beállítása

A kiterjesztett ACL szélesebb körű kezelhetőséget biztosít, mint a normál ACL. A kiterjesztett ACL ugyanis a forrás IP-cím, a cél IP-cím, a protokolltípus és a portszámok alapján engedélyezi vagy tiltja a forgalmat. Mivel a kiterjesztett ACL specifikációja ilyen apró részletekre is kiterjedő lehet, mérete általában gyorsan növekszik. Minél több utasítást tartalmaz egy ACL, annál nehezebben kezelhető.

A kiterjesztett ACL-ek a 100 és 199, illetve a 2000 és 2699 közötti azonosító számokat használják. A normál ACL-re vonatkozó szabályok ugyanúgy vonatkoznak a kiterjesztett ACL-re is:

- Több utasítás is megadható egy ACL-ben.

- Egy ACL minden utasítában ugyanazt az ACL azonositó számot kell megadni.
- Az IP-címek specifikálásakor használhatók a host és az any kulcsszavak.

A leglényegesebb eltérés a kiterjesztett ACL szintaktikájában az, hogy az engedélyező vagy tiltó feltétel után egy protokoll megadása kötelező. Ez a protokoll akár az IP is lehet ha a teljes IP-forgalom tiltása vagy engedélyezése a cél de lehet az IP forgalom egy kiválasztott részhalmazát képező más protokoll (pl. a TCP, az UDP, az ICMP és az OSPF) is.

```
R2(config)#access-list 105 permit tcp 192.168.5.0 0.0.0.255 host 172.16.5.254 eq http
```

Cél IP-cím

Azonosítja a csomagok céljának IP-címét. Ez az érték lehet:

- egy egyedi állomáscím
- állomáscímek egy tartománya
- A host paraméter
- Az any paraméter

```
R2(config)#access-list 105 permit tcp 192.168.5.0 0.0.0.255 host 172.16.5.254 eq http
```

Illeszkedési feltétel

Meghatározza, hogy mely mezőknek kell illeszkedni (egyenlő, nagyobb, kisebb, stb.) az alkalmazásra.

```
R2(config)#access-list 105 permit tcp 192.168.5.0 0.0.0.255 host 172.16.5.254 eq http
```

Feltétel

Meghatározza, hogy egy csomagot engedélyezni vagy tiltani kell.

```
R2(config)#access-list 105 permit tcp 192.168.5.0 0.0.0.255 host 172.16.5.254 eq http
```

Forrás IP-cím

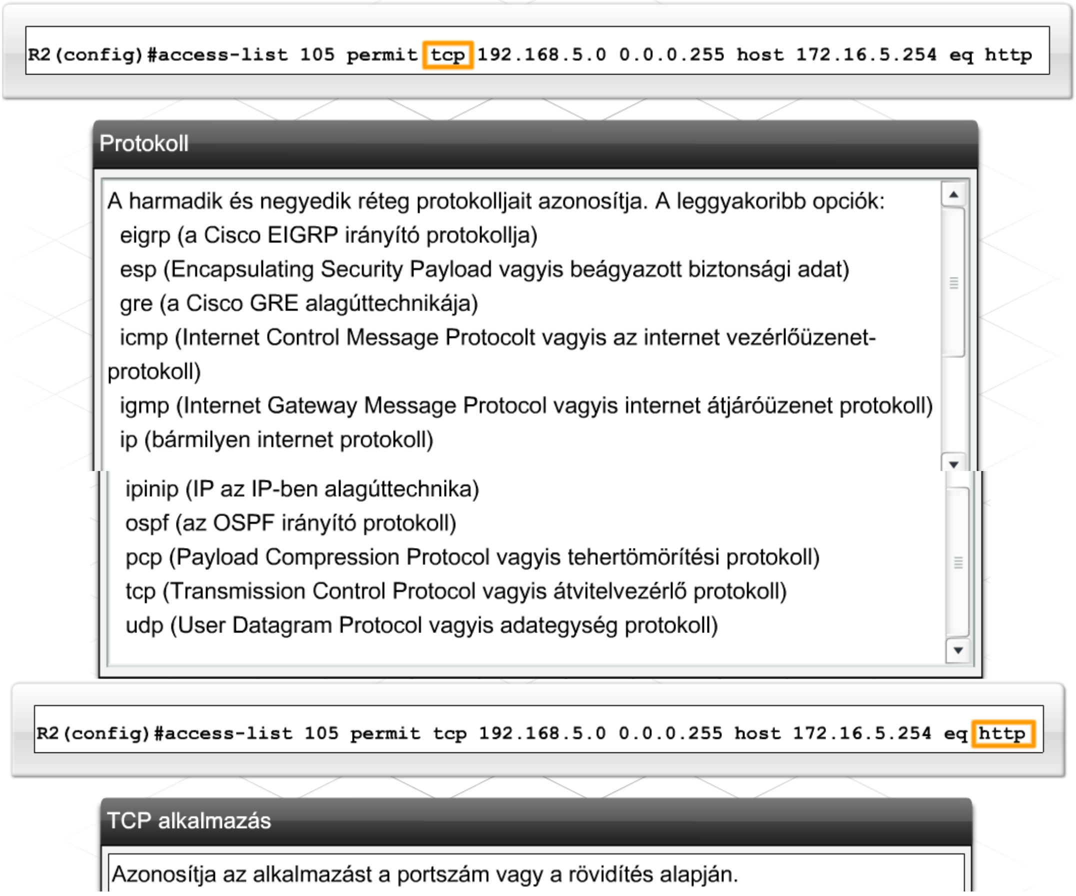
Azonosítja a csomag forrásának IP-címét. Ez az érték lehet:

- egy egyedi állomáscím
- állomáscímek egy tartománya
- A host paraméter
- Az any paraméter

```
R2(config)#access-list 105 permit tcp 192.168.5.0 0.0.0.255 host 172.16.5.254 eq http
```

Az ACL száma

Az ACL-t egy egyedi szám alapján azonosítja. A normál ACL az 1 és 99, valamint az 1300 és 1999 közötti számokat használja. A kiterjesztett ACL a 100 és 199, valamint a 2000 és 2699 közötti számokat használja.



Az elvárások teljesítése gyakran többféle módon is lehetséges.

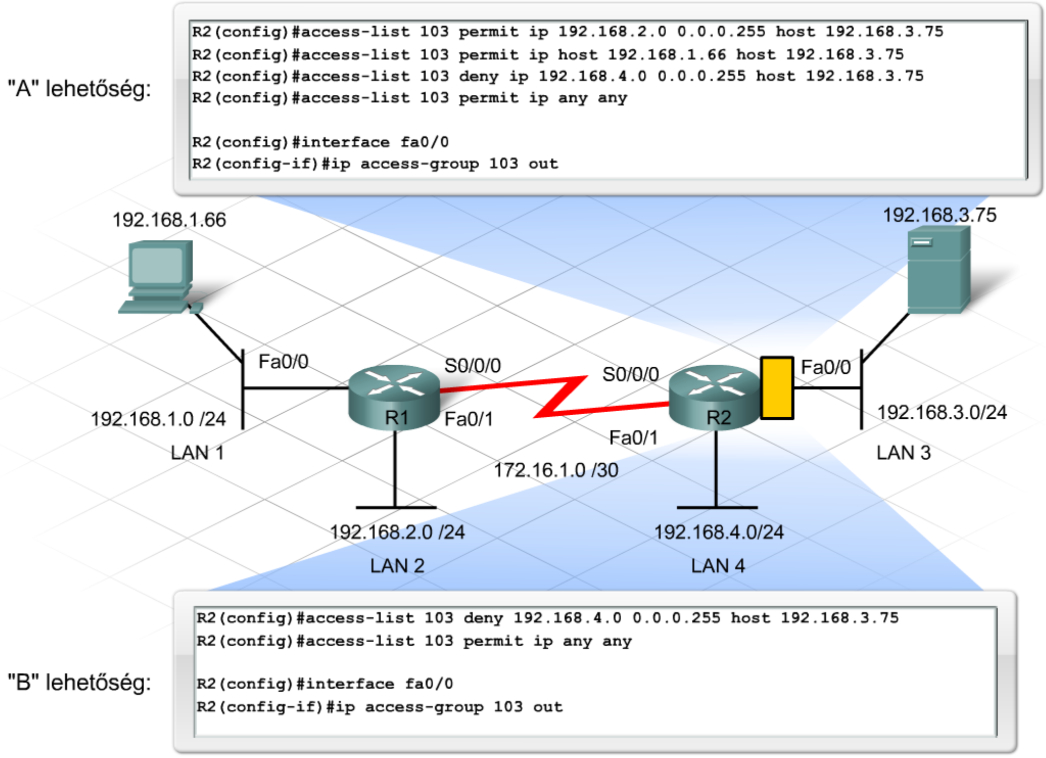
Ha egy vállalatnak van egy 192.168.3.75 címen elérhető kiszolgálója akkor ennek elérésére vonatkozóan például az alábbi elvárások lehetségesek:

- A 192.168.2.0 LAN állomásai számára engedélyezzük a kiszolgáló elérését!
- A 192.168.1.66 állomás számára engedélyezzük kiszolgáló elérését!
- Tiltsuk meg a 192.168.4.0 LAN állomásai számára a kiszolgáló elérését!
- A vállalaton belül mindenki másnak engedélyezzük a kiszolgáló elérését!

Legalább két lehetséges megoldás van, amely a fenti elvárásoknak megfelel. Az ACL tervezésekor törekedjünk arra, hogy a lehetőségekhez mérten minél kevesebb utasítással oldjuk meg a problémát!

Az utasítások számának minimalizálása és a forgalomirányító feldolgozási terhelésének csökkentése többek között az alábbi módon lehetséges:

- Nagy forgalom vizsgálatát és a nem engedélyezett forgalom tiltását az ACL elején végezzük! Ez a megközelítésmód garantálja, hogy itt kiejtett a csomagokat nem kell az ACL későbbi részének utasításaival összevetni.
- Tartományok használatával vonjunk össze több engedélyező, illetve tiltó utasítást egyetlen utasításba!
- Fontoljuk meg egy bizonyos csoport tiltását a vele ellentétes elbírálású, nagyobb csoport engedélyezése helyett!



8.3.5 A nevesített ACL beállítása

A Cisco IOS 11.2 vagy annál újabb verzióiban már lehetséges nevesített ACL (NACL) létrehozása. Az NACL esetében a normál és a kiterjesztett ACL-ekhez használatos számtartományokat beszédes név váltja fel. A nevesített ACL a normál és a kiterjesztett ACL minden funkciójával és előnyével rendelkezik, csupán a létrehozásához használt szintaktika eltérő.

Az ACL-hez rendelt név egyedi. A csupa nagybetűvel megadott név könnyebben felismerhető a forgalomirányító parancskimenetében és a hibaelhárítás során.

Nevesített ACL az alábbi paranccsal hozható létre:

```
ip access-list {standard | extended} név
```

A fenti parancs kiadása után a forgalomirányító az NACL konfigurációs almódba vált. A kezdeti névmegadási parancs után egyesével vigyük be az összes engedélyező és tiltó utasítást! Az NACL a normál vagy a kiterjesztett ACL permit vagy deny utasítással kezdődő parancsformátumát használja.

A nevesített ACL hozzárendelése egy interfészhez úgy történik, mint a normál és a kiterjesztett ACL-ek esetében, csak itt név azonositja az interfészhez kapcsolt ACL-t.

Egy nevesített ACL megfelelő szintaktikáját, az utasítások sorrendjét és az interfészeken történő elhelyezését a normál ACL esetében is használt parancsokkal ellenőrizhetjük.

```
R1(config)#ip access-list extended SALES-ONLY
R1(config-ext-nacl)#permit ip 192.168.1.66 0.0.0.0 any
R1(config-ext-nacl)#permit ip 192.168.1.77 0.0.0.0 any

R1(config)#interface fa0/0
R1(config-if)#ip access-group SALES-ONLY in
```

Az IOS régebbi verzióiban az ACL átszerkesztéséhez az alábbiakra volt szükség:

- Az ACL kimásolása egy szövegszerkesztőbe.
- Az ACL eltávolítása a forgalomirányítóról.
- Az ACL ismételt létrehozása, majd a szerkesztett változat alkalmazása.

Sajnos a fenti folyamat a szerkesztési ciklus végéig minden forgalmat átenged az interfészen, így a hálózat védtelen marad a lehetséges biztonsági résekkel szemben.

Az IOS jelenlegi verzióiban a számozott és a nevesített ACL-ek szerkesztéséhez használjuk az `ip access-list` parancsot! Az ACL-ek sorai számozva (10, 20, 30, stb.) jelennek meg. A sorokhoz tartozó számok megtekintéséhez használjuk az alábbi parancsot:

`show access-lists`

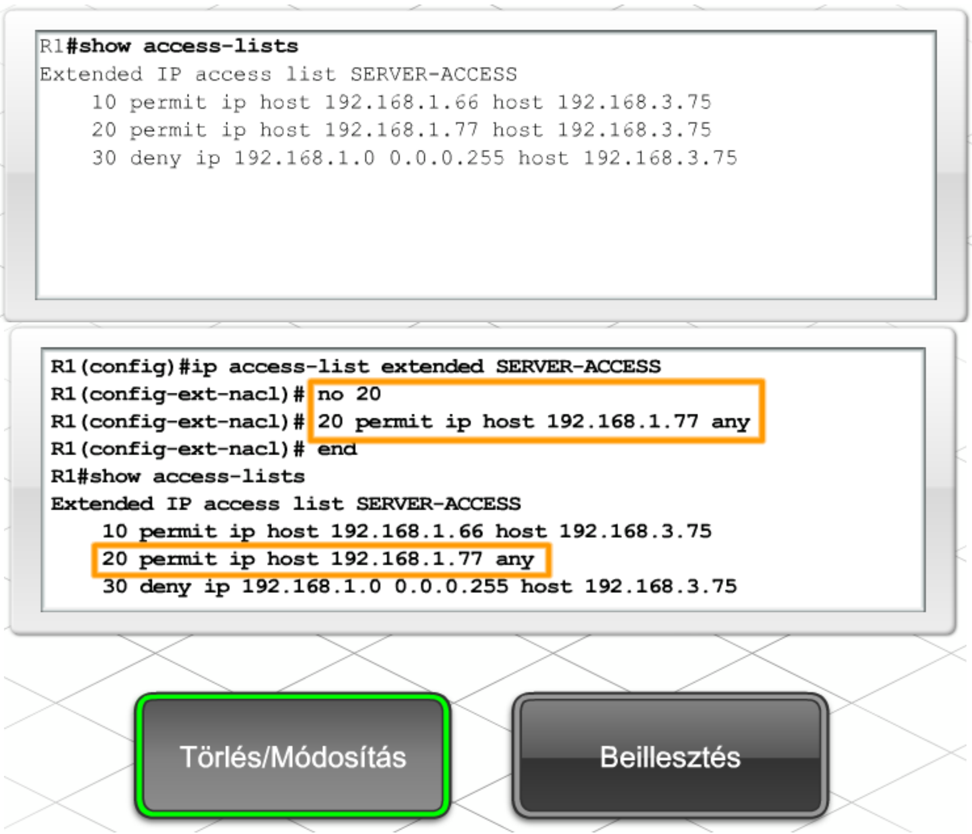
Egy már létező sor szerkesztéséhez az alábbiakat kell tenni:

- A no line number parancs használatával távolítsuk el a sort!
- A sorhoz tartozó szám használatával adjuk ismét hozzá ugyanazt a sort az ACL-hez!

A 20-as és 30-as sorok közé egy új sor beillesztéséhez:

- Adjuk ki a két meglévő sor közé eső számmal (pl.: 25) kezdődő új ACL utasítást!

Az újrarendezett és 10-esével újraszámozott sorok megtekintéséhez adjuk ki a `show access-lists` parancsot!



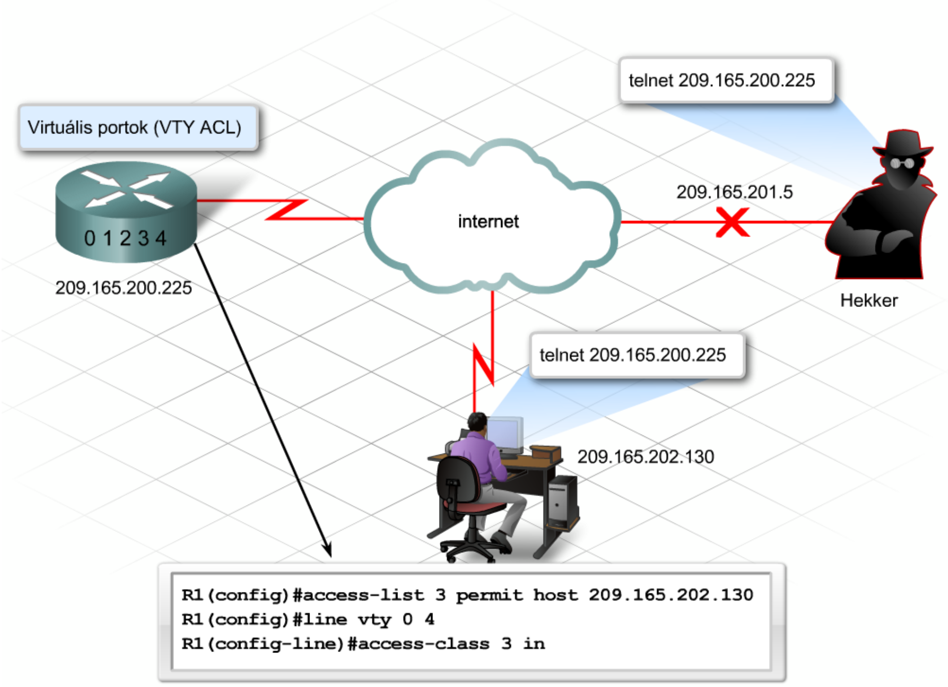
```
R1(config)#ip access-list extended SERVER-ACCESS
R1(config-ext-nacl)# 25 deny ip host 192.168.1.88 any
R1(config-ext-nacl)# end
R1#show access-lists
Extended IP access list SERVER-ACCESS
    10 permit ip host 192.168.1.66 host 192.168.3.75
    20 permit ip host 192.168.1.77 any
    25 deny ip host 192.168.1.88 any
    30 deny ip 192.168.1.0 0.0.0.255 host 192.168.3.75
```

8.3.6 A virtuális terminál alapú hozzáférés beállítása a forgalomirányítón

A hálózati rendszergazdának gyakran kell konfigurálnia távoli telephelyen lévő forgalomirányítókat. A távoli forgalomirányítóra történő bejelentkezéshez a Telnet, a Secure Shell (SSH) vagy ezekhez hasonló ügyfélprogramok használhatók. A Telnet nem túl biztonságos, mivel a felhasználói nevet és a jelszót egyszerű szöveges formában továbbítja. Az SSH ezzel szemben mindkét adatot titkosított formában küldi tovább.

Amikor a hálózati rendszergazda a Telnet ügyfélprogram használatával egy távoli forgalomirányítóhoz kapcsolódik, akkor a forgalomirányító szemszögéből egy bejövő kapcsolat kezdeményezése történik. A Telnet és az SSH egyaránt sávon belüli hálózat-felügyeleti eszköz, ezért szüksége van az IP-protokollra és a forgalomirányítóhoz vezető működő hálózati kapcsolatra.

A virtuális terminál (VTY) alapú hozzáférés korlátozásának célja a hálózatbiztonság javítása. A külső támadók megpróbálhatnak hozzáférést szerezni a forgalomirányítóhoz. Ha a forgalomirányító virtuális portján nincs hozzáférési lista, akkor bárki bejuthat, aki a Telnet felhasználói nevét és jelszavát ismeri. Amennyiben a forgalomirányító vty portjához rendelt ACL kizárólag meghatározott IP-címeket engedélyez, akkor az ACL-ben nem engedélyezett IP-címről, a telnet segítségével kapcsolódni próbáló bármilyen személy hozzáférését megtagadja a forgalomirányító. Ugyanakkor azt se feledjük, hogy ez problémát okozhat, ha a rendszergazdának különböző helyekről és IP-címekről kell a forgalomirányítóhoz kapcsolódni.

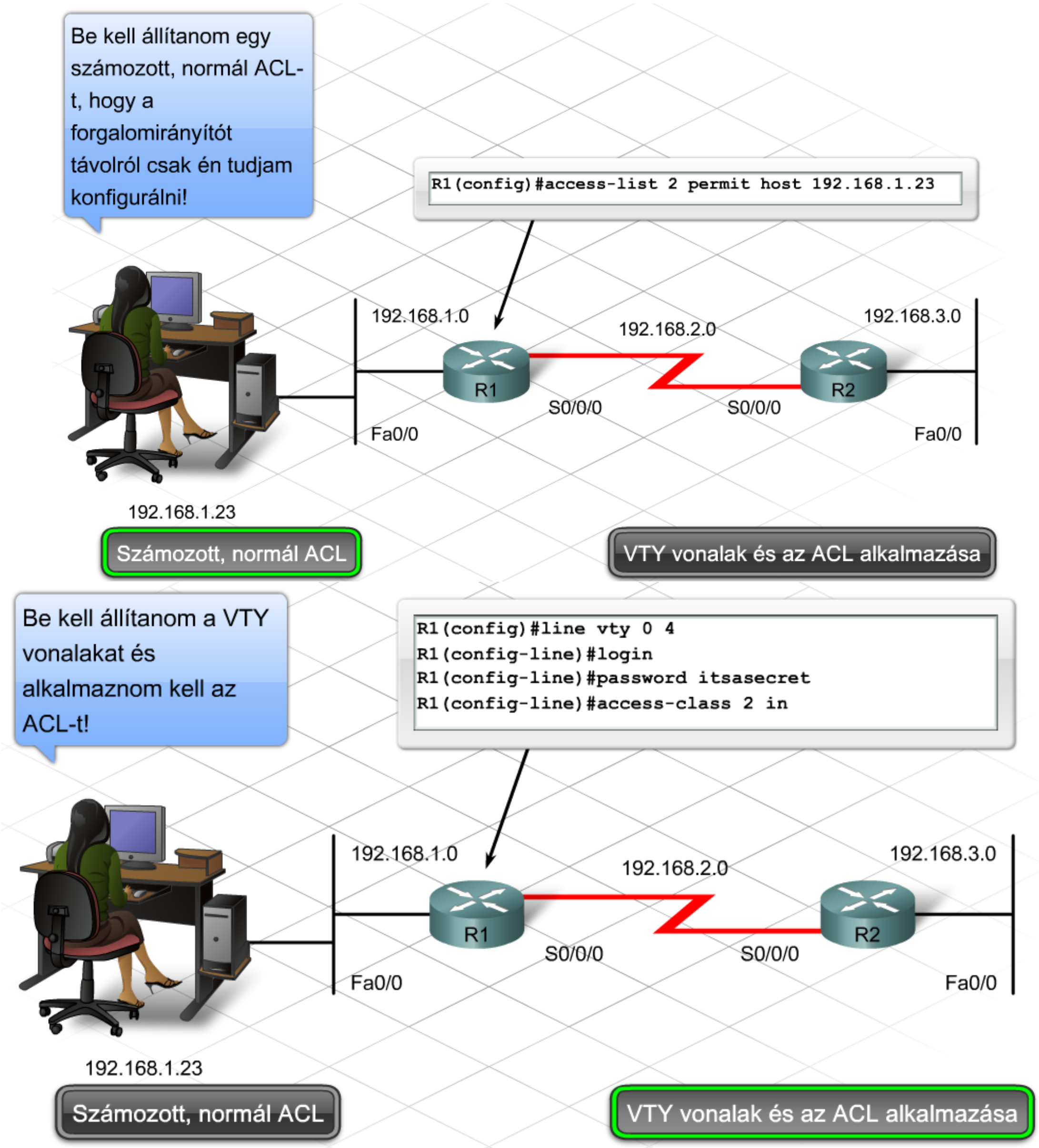


A virtuális terminál alapú hozzáférési lista létrehozásának folyamata ugyanaz, mint egy normál interfészhez kapcsolódó ACL esetén. Ezzel szemben az ACL hozzárendelése egy vagy több VTY vonalhoz más paranccsal történik. Az ip access-group parancs helyett az access-class parancsot kell használnunk.

A VTY vonalakhoz hozzárendelt hozzáférési listák beállításához kövessük az alábbi irányelveket:

- A VTY vonalakhoz ne nevesített, hanem számozott ACL-t használjunk!
- A korlátozásokat minden VTY vonalhoz hozzá kell rendelni, mivel nem szabályozható, hogy a felhasználó melyik vonalon kapcsolódjon!

A VTY kapcsolat a Telnet ügyfélprogram és a célként megadott forgalomirányító Telnet szerverprogramja között jön létre. A hálózati rendszergazda létrehozza a kapcsolatot a célként megadott forgalomirányítóval, megadja felhasználói nevét és jelszavát, majd elvégzi a szükséges konfigurációs változtatásokat.



8.4 Meghatározott forgalomtípusok engedélyezése és tiltása

8.4.1 ACL-ek beállításának alkalmazása- és portszűrése

A kiterjesztett ACL általában a forrás- és a cél IP-cím alapján szűr. A szűrés anonban ennél specifikusabb csomagjellemzők alapján is elvégezhető. Az OSI 3. rétegbeli hálózati protokollja, valamint a 4. rétegbeli szállítási protokollok és az alkalmazásportok lehetővé teszik az ilyen jellegű szűrést.

A szűréshez rendelkezésre álló protokollok között szerepel az IP, a TCP, az UDP és az ICMP.

A kiterjesztett ACL a célport száma alapján is végez szűrést. Ezek a portszámok írják le a csomag által elérni kívánt alkalmazást, ill. szolgáltatást. Minden alkalmazáshoz egy rögzített portszám tartozik.

A forgalomirányítónak meg kell vizsgálnia az Ethernet keret szállitmányát, hogy az ACL-ekkel történő összehasonlításhoz kigyűjtse a szükséges IP-címeket és portszámokat.

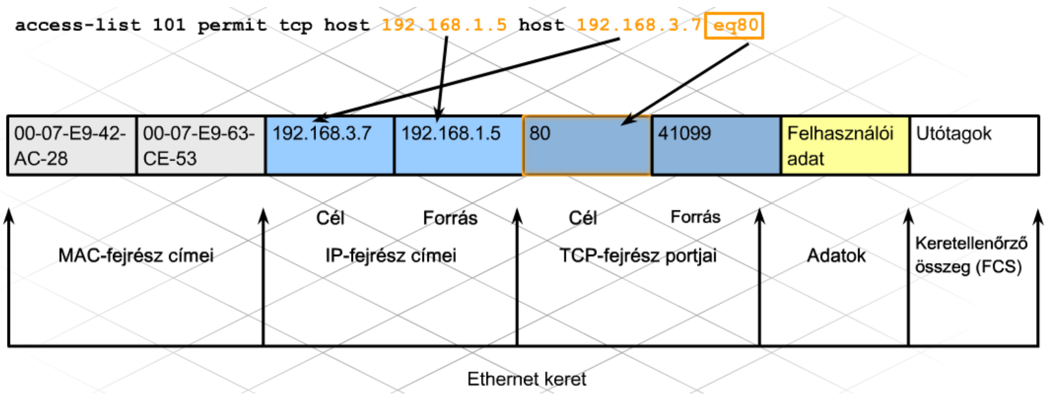
Az utasítás kiértékelése előtt a portszámokon kívül egy feltétel megadása is szükséges. Erre az alábbi gyakori rövidítések használatosak:

- **eq** - egyenlő (equals)
- **gt** – nagyobb, mint (greater than)
- **lt** – kisebb, mint (less than)

Vegyük az alábbi példát:

```
R1(config)#access-list 122 permit tcp 192.168.1.0 0.0.0.255 host
192.168.2.89 eq 80
```

A fenti ACL utasítás engedélyezi a 192.168.1.0 hálózatból származó, a 80-as porton HTTP-hozzáférést igénylő forgalmat. Amennyiben egy felhasználó telnet- vagy FTP-kapcsolatot próbál létesíteni a 192.168.2.89 című állomással, a minden hozzáférési lista végén megtalálható implicit tiltó utasítás megakadályozza azt.



Egy konkrét alkalmazás alapján történő szűréshez ismernünk kell az adott alkalmazás portszámát. Az alkalmazásokat egy portszám és egy név azonositja. Egy ACL például hivatkozhat akár a 80-as portra, akár a HTTP névre.

Amennyiben sem az alkalmazáshoz tartozó portszám, sem pedig a név nem ismert, próbáljuk megtalálni az információt az alábbi lépések valamelyikével:

1. Keressünk fel egy IP-címek bejegyzésével foglalkozó oldalt (pl.: http://www.iana.org) a világhálón!
2. Nézzünk utána a szoftver dokumentációjában!
3. Látogassunk el a szoftvergyártó weboldalára!
4. Szerezzük meg az adatokat egy csomagvizsgáló (packet sniffer) segítségével közvetlenül az alkalmazásból!
5. Használjuk a ? lehetőséget az `access-list` parancshoz! Az így kapott lista tartalmazza a TCP protokollhoz tartozó legismertebb portneveket és portszámokat.

Néhány alkalmazás egynél több portszámot használ. Például, az FTP adatátvitel a 20-as porton történik, de az FTP-t lehetővé tevő kapcsolatvezérlés a 21-s portot használja. Az FTP forgalom teljes tiltásához mindkét portot le kell tiltanunk!

Több portszám megfelelő kezeléséhez a Cisco IOS ACL-ek képesek port-tartományok alapján is szűrni. Ehhez használjuk az ACL utasítás gt, lt vagy range operátorát! A két FTP-t tiltó ACL utasítás például összevonható az alábbi paranccsal:

```
R1(config)#access-list 181 deny tcp any 192.168.77.0 0.0.0.255 range 20 21
```

```
R1(config)#access-list 101 permit tcp host 192.168.1.1 host 192.168.2.89 eq ?
 <0-65535>  Port number
 (**kimenet elhagyva**)
 bgp       Border Gateway Protocol (179)
 domain    Domain Name Service (53)
 echo      Echo (7)
 ftp       File Transfer Protocol (21)
 ftp-data       FTP data connections (20)
 ident     Ident Protocol (113)
 irc       Internet Relay Chat (194)
 pop3      Post Office Protocol v3 (110)
 smtp      Simple Mail Transport Protocol (25)
 telnet    Telnet (23)
 www       World Wide Web (HTTP, 80)
```

8.4.2 Az ACL-ek beállítása a kapcsolat-felvétel utáni forgalom támogatásához

Az ACL-eket gyakran azért használunk, hogy védelmet nyújtsanak a belső hálózat számára a külső forrásokkal szemben. Ugyanakkor a belső hálózat védelme mellett a belső felhasználók számára biztosítani kell a hozzáférést minden erőforráshoz. Amikor a belső felhasználók külső erőforrásokat használnak, az általuk igényelt erőforrásoknak át kell jutniuk az ACL-en. Ha például egy belső felhasználó kapcsolódni akar egy külső webkiszolgálóhoz, az ACL-nek engedélyeznie kell a bentről kért kűlső html csomagok bejutását. Mivel az ACL-ek végén mindig ott szerepel az implicit tiltás, a fenti erőforrásokat külön engedélyezni kell az ACL-ben. A minden lehetséges igényelt erőforrást engedélyező különálló utasítások hosszú ACL-t és biztonsági réseket eredményezhetnek.

A probléma megoldható egyetlen utasítás megadásával, amely a belső felhasználók számára engedélyezi egy TCP kapcsolat felépítését a külső erőforrásokhoz. Amint megtörtént a TCP háromfázisú kézfogása és a kapcsolat létrejött, a két eszköz között küldött összes csomag engedélyezve lesz. Ehhez használjuk az established kulcsszót!

```
access-list 101 permit tcp any any established
```

A fenti utasítás használatával az összes kívülről érkező tcp csomag engedélyezve lesz, feltéve, ha a válasz egy belülről érkező kérésre jött. A bentről kezdeményezett kommunikáció eredményeként beérkező válaszcsomagok engedélyezése az állapottartó csomagvizsgálat (Stateful Packet Inspection, SPI) egyik formája.

A már létrejött forgalmon kívül arra is szükség lehet, hogy egy belső felhasználó külső eszközöket pingelhessen. Ugyanakkor nem kívánatos, hogy külső felhasználók megpingelhessék a belső hálózat eszközeit vagy követhessék az azokhoz vezető útvonalat. Ilyen esetekben használható az ACL utasításban megadott echo-reply és az unreachable kulcsszó a ping válaszok és a cél elérhetetlenségét jelző üzenetek fogadásának engedélyezésére. Ugyanakkor a külső forrásokból származó ping mindaddig el lesz utasítva, amíg azt egy másik utasítás külön nem engedélyezi.

8.4.3 A NAT és a PAT szerepe az ACL-ek elhelyezésébeb

Az ACL-ek megtervezésénél gondot okozhat a hálózati címfordítás (NAT) és a portcímfordítás (PAT) használata. Külön figyelmet igényel a rendszergazdától, ha egy olyan interfészen alkalmaz ACL-t, amin egyébként címfordítás is történik.

Ha egy forgalomirányítón címfordítást és ACL-t együtt használunk, legyünk tisztában ezek együttműködésének módjával!

1. Ha egy bejövő csomag érkezik a címfordítást végző külső interfészre, akkor a forgalomirányító:

- Alkalmazza a bejövő ACL-t.
- A célcímet külsőről belsőre (globálisról lokálisra) fordítja.
- Továbbítja a csomagot.

2. Ha egy csomag kifelé távozik a címfordítást végző külső interfészről, akkor a forgalomirányító:

- A forráscímet belsőről külsőre (lokálisról globálisra) fordítja. Alkalmazza a kimenő ACL-t.
- Alkalmazza a kimenő ACL-t.

Az ACL-t úgy tervezzük meg, hogy a címfordításhoz való viszonyától függően vagy csak a privát, vagy csak a publikus címeket szűrje! Amennyiben a címfordítást végző külső interfészre bejövő vagy onnan kimenő forgalomról van szó, akkor a publikus címeket kell szűrni.

8.4.4 A hálózati ACL-ek és elhelyezésük elemzése

A hálózati rendszergazdának még a tényleges használat előtt meg kell vizsgálnia az ACL minden utasításának hatását. Egy interfészhez rendelt, de rosszul megtervezett ACL azonnali problémákhoz vezethet. Ezek a problémák a hamis biztonságérzettől, a forgalomirányító felesleges terhelésén keresztül, a működésképtelen hálózatig terjedhetnek.

A rendszergazdának sorról sorra át kell néznie az ACL-t, és utasitásonként meg kell válaszolni az alábbi kérdéseket:

- Mely szolgáltatásokat tiltja az utasítás?
- Mi a forrás, és mi a cél?
- Mely portszámokat tiltja?
- Mi történne, ha az ACL-t áthelyeznénk egy másik interfészre?

- Mi történne, ha az ACL a másik irányú forgalmat szűrné?
- Okoz-e bármiféle problémát a hálózati címfordítás?

Kiterjesztett ACL vizsgálatakor nem szabad megfeledkezni az alábbi kulcsszempontokról:

- A `tcp` kulcsszó az FTP, a HTTP, a Telnet és hasonló protokollokat engedélyezi vagy tiltja.
- A `permit ip` kulcskifejezés a teljes IP-forgalmat – beleértve a TCP, az UDP és az ICMP protokollt – engedélyezi.

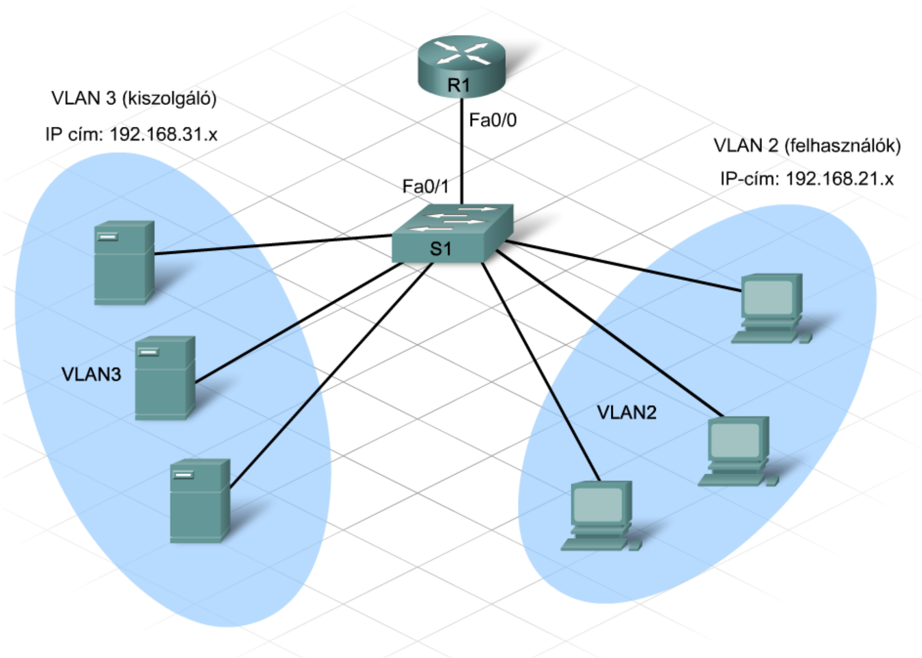
8.4.5 Az ACL-ek beállítása a VLAN-ok közötti forgalomirányításhoz

Ha egy hálózatban VLAN-ok közötti forgalomirányítást használunk, esetenként szükség lehet az egyik VLAN-ból a másikba tartó forgalom ACL-ekkel történő vezérlésére.

Az ACL-eket rendeljük közvetlenül a forgalomirányító VLAN interfészeihez vagy alinterfészeihez éppen úgy, mint a fizikai interfészek esetében!

A vállalati hálózatokban a kiszolgálók általában a felhasználói csoportoktól eltérő VLAN-ban kapnak helyet. Ilyen esetekben a kiszolgálói VLAN-hoz való hozzáférés szűrést igényel.

Az alinterfészekre helyezett ACL-ek létrehozására és használatára ugyanazok a szabályok és irányelvek vonatkoznak, mint a fizikai interfészre helyezettek esetében.



8.5 Forgalomszűrés, hozzáférési alkalmazásával

8.5.1 A naplózás használata az ACL funkcionalitásának ellenőrzésére

Egy ACL megírása és interfészhez rendelése után a hálózati rendszergazdának érdemes megvizsgálnia az egyezések számát. Egyezésről beszélünk, ha egy bejövő csomag mezői megfelelnek az ACL összes viszonyítási mezőjének. Az egyezések számának megtekintése segít annak megítélésében, hogy az ACL utasítások elérik-e a kívánt hatást.

Az ACL utasítások alapértelmezés szerint rögzítik az egyezések (találatok) számát, amelyet megjelenítenek az érintett utasítások végén. Az egyezések megtekintéséhez használjuk az alábbi parancsot:

```
show access-list
```

A show `access-list` parancs használatával ACL soronként megjelenített egyezési számértékek utasításonként megmutatják, hány csomag-egyezés történt. A kimenet a csomag forrását vagy célját, sem pedig a használt protokollt nem jelzi.

Az engedélyezett vagy elutasított csomagokkal kapcsolatos további részletek megismeréséhez aktiváljuk a naplózás folyamatát! A naplózás az egyes ACL utasításokra külön-külön aktiválható, a vizsgálni kívánt utasítások végére illesztett log opcióval.

A naplózást csak rövid időre, az ACL tesztelésének befejezéséig kapcsoljuk be, az események naplózása ugyanis jelentősen növelheti a forgalomirányító terhelését.

A konzolra történő naplózás a forgalomirányító memóriáját használja, ami korlátozott erőforrásnak számít. Ehelyett állítsuk be a forgalomirányítón, hogy a naplózandó információt egy külső kiszolgálóra küldje! Ezek az ún. `syslog` üzenetek lehetővé teszik az információk valós idejű vagy egy későbbi időpontban történő megtekintését.

A syslog esemény-üzenetek nyolc súlyossági szint valamelyikébe sorolhatók. A 0. szint vészhelyzetet vagy használhatatlan rendszert jelent, a 7. pedig információs (pl.: hibakeresési) üzeneteket azonosit.

Az ACL naplózás többek között az alábbi információs üzenetet generálja:

- az ACL száma
- az engedélyezett vagy elutasított csomag
- a forrás- és célcímek
- a csomagok száma

Az üzenet az első csomagegyezés esetén, majd ezt követően 5 percenként generálódik.

A naplózás kikapcsolásához használjuk az alábbi parancsot:

```
no logging console
```

A hibakeresés teljes kikapcsolásához használjuk az alábbi parancsot:

```
undebug all
```

Egy konkrét (pl. IP-csomagokhoz kapcsolódó) hibakeresés kikapcsolásához használjuk az alábbi parancsot:

```
no debug ip packet
```

Naplózási szintek		Fontossági szint <0-7>
riasztások	Azonnali beavatkozás szükséges.	(fontosság=1)
kritikus	Kritikus helyzet.	(fontosság=2)
hibakeresési	Hibakeresési üzenetek.	(fontosság=7)
vészhelyzetek	A rendszer használhatatlan.	(fontosság=0)
hibák	Hibás helyzet.	(fontosság=3)
szűrt	Engedélyezi a szűrt naplózást.	
garantált	Garantálja a konzolüzeneteket.	
tájékoztató	Tájékoztató üzenetek.	(fontosság=6)
értesítések	Normális, de fontos helyzet.	(fontosság=5)
figyelmeztetések	Figyelmeztetési helyzet.	(fontosság=4)
xml	Engedélyezi az XML formátumú naplózást.	

8.5.2 A forgalomirányító naplóinak elemzése

A konzolra történő naplózás a forgalomirányító memóriáját használja, ami korlátozott erőforrásnak számít. Ehelyett állítsuk be a forgalomirányítón, hogy a naplózás kimenetét egy külső kiszolgálóra küldje! Ezek az ún. syslog üzenetek lehetővé teszik az információk valós idejű vagy egy későbbi időpontban történő megtekintését.

A naplózott eseménytípusok az alábbiak állapotát tartalmazzák:

- a forgalomirányító interfészei
- a használt protokollok
- a sávszélesség-használat
- az ACL üzenetek
- a konfigurációs események

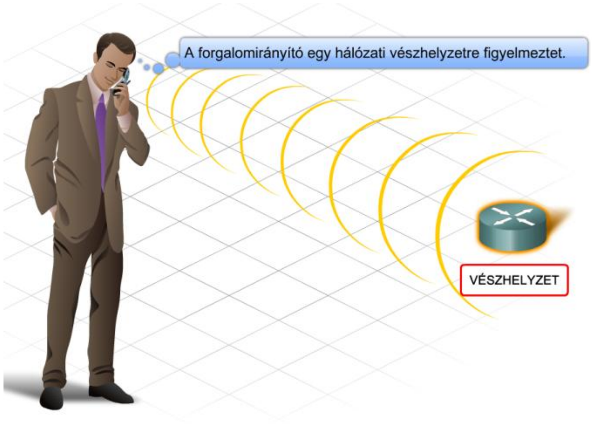
Mindenképpen tanácsos kihasználni azt a lehetőséget, amely egy kritikus esemény bekövetkezésekor e-mailben, személyi hívón vagy mobiltelefonon értesíti a hálózati rendszergazdát.

Az egyéb beállítási lehetőségek között szerepel:

- értesítés az újonnan érkezett üzenetekről
- az üzenetek rendezése és csoportosítása
- az üzenetek súlyossága alapján történő szűrés
- az összes vagy csak a kijelölt üzenetek törlése

Syslog kiszolgálóprogram többféle forrásból is beszerezhető. Ezek tudásszintje és kezelhetősége az ár függvényében változik, de léteznek az interneten elérhető, ingyenes programok is.

A syslog egy olyan protokoll, amelyet minden hálózati berendezés – ideértve a kapcsolókat, forgalomirányítókat, tűzfalakat, tárolórendszereket, modemeket, vezeték nélküli eszközöket és UNIX állomásokat – támogat.



Egy syslog kiszolgáló használatához telepítsük a programot egy Windows, Linux, UNIX vagy MAC OS operációs rendszert futtató kiszolgálóra, majd állítsuk be a forgalomirányítón, hogy a naplózott eseményeket erre a syslog kiszolgálóra küldje!

Az alábbi példában szereplő parancs egy syslog kiszolgálót futtató állomás IP-címét használja:

```
logging 192.168.3.11
```

Egy probléma elhárítása során mindig állítsuk be az időbélyeg szolgáltatást a naplózáshoz! Bizonyosodjunk meg arról, hogy a forgalomirányítón a dátum és idő be legyen állítva, és így a naplóállományok mindig a megfelelő időbélyeget jelenítsék meg!

A dátum és idő beállításainak ellenőrzéséhez használjuk a show clock parancsot!

```
R1>show clock
*00:03:45.213 UTC Mon Mar 1 2007
```

A pontos idő beállításához először adjuk meg a Greenwich-i középidőhöz (GMT) viszonyított időzónát, majd állítsuk be az időt! Figyeljünk oda, hogy az idő beállítását (clock set) végző parancsot nem a konfigurációs módban kell kiadni!

Az időzóna beállításához:

```
R1(config)#clock timezone CST -6
```

Az idő beállításához:

```
R1#clock set 10:25:00 Sep 10 2007
```



8.5.3 Bevált ACL megoldások

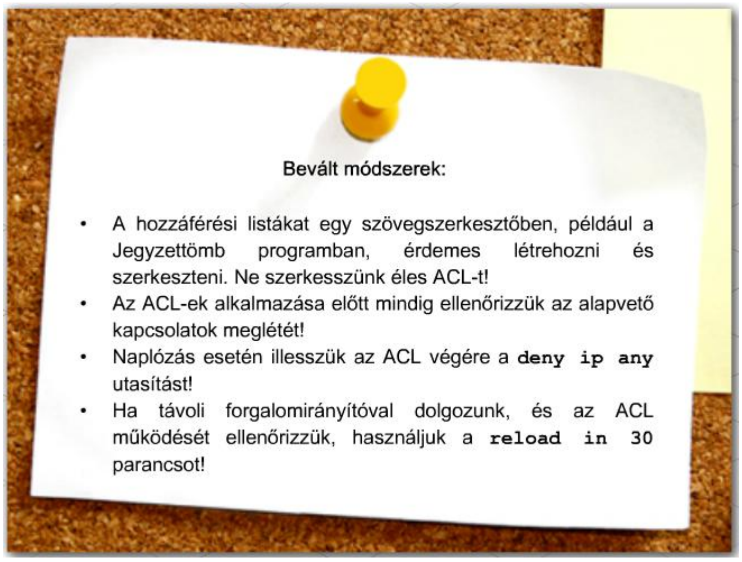
Az ACL nagyon hatékony szűrési eszköz. Egy ACL azonnal aktívvá válnak, amint alkalmazzuk egy interfészre.

Sokkal jobban járunk, ha több időt töltünk az ACL megtervezésével és hibaelhárításával még a tényleges használat megkezdése előtt, mintha utána próbálnánk megtalálni és kijavítani a problémákat!

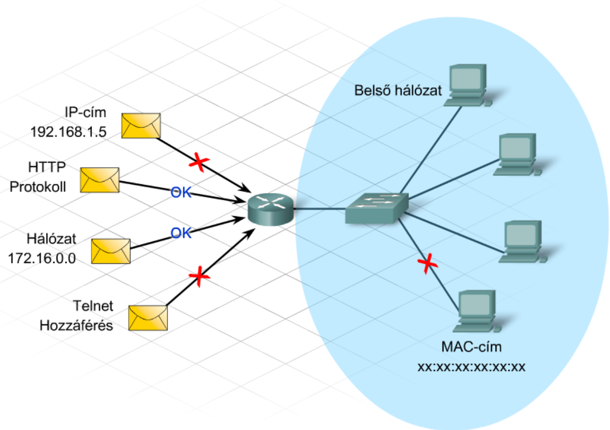
Az ACL-ek alkalmazása előtt mindig ellenőrizzük a teljeskörű kapcsolatok meglétét! Amennyiben egy állomás pingelése hibás kábel vagy valamilyen IP-beállítási probléma miatt sikertelen, az ACL nehezebbé teheti a hiba elhárítását.

Naplózás esetén az ACL utolsó sorába irjuk be a `deny ip any` utasítást, így nyomon követhetjük az elutasított csomagok számát!

Ha távoli forgalomirányítóval dolgozunk, és az ACL működését ellenőrizzük, használjuk a `reload in 30` parancsot! Ha ugyanis egy esetleges hiba az ACL-ben letiltja a hozzáférést a forgalomirányítóhoz, a távoli kapcsolat is megszűnhet. A fenti parancs használatával a forgalomirányító 30 perc elteltével újraindul az ACL nélküli indítási konfiguráció beállításaival. Amikor már elégedettek vagyunk az ACL működésével, másoljuk az aktív konfigurációt az indítási konfigurációba!



8.6 A fejezet összefoglalása



- A forgalomszűrés a csomag tartalmának elemzési folyamata annak meghatározására, vajon a csomag átengedhető-e vagy sem.
- Az ACL-ekkel felügyelhető a hálózati forgalom. Biztonságossá tehető mind a kimenő, mind a bejövő hálózatelérés, illetve védhetők a hálózati erőforrások.
- Három ACL típus létezik: normál, kiterjesztett és nevesített.
- Az ACL-ek a forgalmat a forrás és a cél IP-címe, az alkalmazás és a protokoll alapján szűrik.
- Alkalmazzon egy ACL-t a forgalomirányító egyik interfészére, és vizsgálja meg a bejövő vagy kimenő csomagokat!

- A helyettesítő maszkok használata rugalmasságot biztosít, így egyetlen utasítással tiltható egy címtartomány vagy egy egész hálózat.
- A helyettesítő maszk a bejövő cím és egy összehasonlítási cím összevetésével meghatározza, hogy mely cimeknek kell azonosnak lenni.
- A helyettesítő maszk meghatározásához vonja ki a címre vagy tartományra vonatkozó decimális alhálózati maszkot a csupa 255-ből álló (255.255.255.255) maszkból.
- Minden ACL végén van egy implicit **`deny any`** utasítás.
- Az **`any`** kulcsszó az összes állomásra, a **`host`** kulcsszó pedig az egyedi IP-címekre vonatkozik.

Az egyetlen állomást engedélyező helyettesítő maszkok:
```
172.16.22.87 0.0.0.0
host 172.22.8.17
```
Egy /24 hálózat állomásainak egy tartományát engedélyező helyettesítő maszk:
```
172.16.22.0 0.0.0.255
```
Egy egész /16 hálózatot engedélyező helyettesítő maszk:
```
172.16.0.0 0.0.255.255
```
Egy egész /8 hálózatot engedélyező helyettesítő maszk:
```
10.0.0.0 0.255.255.255
```



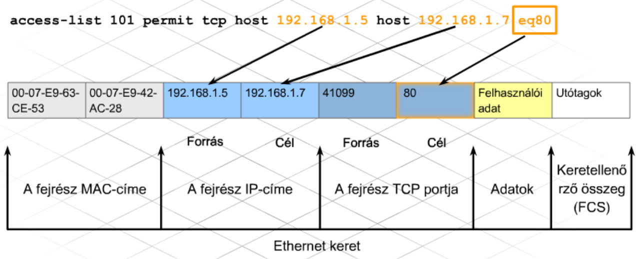
ACL feldolgozási és létrehozási irányelvek

- Irányonként és protokollonként egy hozzáférési listát lehet létrehozni.
- A normál ACL-eket a célhoz a lehető legközelebb kell elhelyezni.
- A kiterjesztett ACL-eket a forráshoz a lehető legközelebb kell elhelyezni.
- Mindig a lista típusának megfelelő számtartományt kell használni.
- A bejövő vagy kimenő irány meghatározásához az interfészt mindig a forgalomirányító szemszögéből kell nézni.
- Az utasítások feldolgozása egymás után, felülről lefelé haladva történik.
- Amennyiben egy csomagra nincs illeszkedés, eldobásra kerül.
- A hozzáférési lista utasításait mindig a konkréttól az általános felé haladva kell megadni.
- Az ACL-ben mindig szerepeljen egy permit utasítás, máskülönben minden forgalom tiltásra kerül.

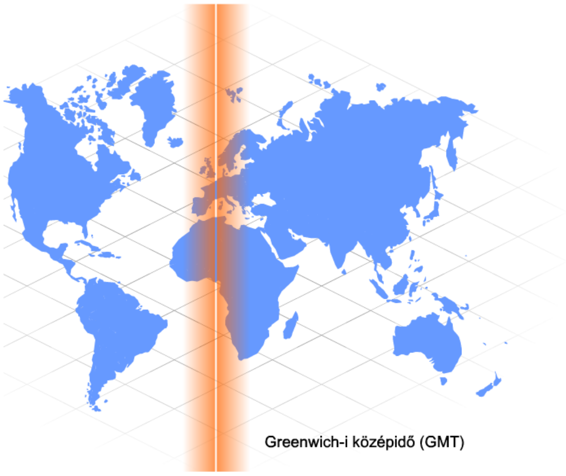
- A normál ACL-ek csak egy forrás IP-cím alapján képesek szűrni, így azokat a célhoz legközelebb kell elhelyezni.
- A kiterjesztett ACL a forrás és cél IP-címe, a protokoll és a portszámok alapján is szűrhet, és a forráshoz legközelebb érdemes elhelyezni.
- Az ACL típusa és a követelmények alapján határozza meg az ACL helyét!
- Minden interfészhez irányonként és protokollonként egy ACL adható meg.
- Hozzon létre egy egyedi azonosítóval rendelkező ACL-t, majd az **`ip access-group`** parancs segítségével alkalmazza egy interfészre, bejövő vagy kimenő irányba!
- A **`show ip interface`**, **`show access-lists`** és **`show running-config`** parancsok segítségével a hálózati rendszergazda megtekintheti a forgalomirányítón beállított összes ACL-t.
- A nevesített ACL a normál és kiterjesztett ACL-ek minden funkcióját és előnyeit kínálja.
- A hálózatbiztonság javítása érdekében a VTY hozzáférés ACL-ekkel korlátozható. Egy VTY ACL alkalmazásához az **`access-class`** parancs használható.

8. Forgalomszűrés hozzáférési listák használatával

- A kiterjesztett ACL a forrás és cél IP-címe, a protokoll és a portszámok alapján is szűrhet.
- Az ACL-ek porttartomány alapján történő szűrése a **`gt`**, **`lt`** vagy **`range`** operátorokkal lehetséges.
- A kérésre választ küldő forgalom engedélyezéséhez az established paramétert kell használni.
- A megírt utasítások sorrendje hatással van a forgalomirányító teljesítményére.
- Az ACL-ek megírásánál két megközelítésmód lehetséges: a konkrét forgalom engedélyezése először, majd az általános forgalom tiltása, vagy a konkrét forgalom tiltása először, majd az általános forgalom engedélyezése.
- Az ACL-ek létrehozása és alkalmazása során a címfordítás biztosítása a hálózati rendszergazda felelőssége.
- Az ACL-eket közvetlenül a VLAN logikai interfészekre kell alkalmazni, csakúgy mint a fizikai interfészek esetében.



- Minden ACL utasításra bizonyos számú illeszkedés történik. Ez a szám minden érintett utasítás végén szerepel.
- A naplózás további részleteket nyújt az engedélyezett vagy tiltott csomagokról. A naplózás aktiválásához minden ACL utasítás végéhez hozzá kell adni a log kapcsolót.
- A **`deny ip any any log`** hozzáadásával követhető azon csomagok száma, amelyek nem illeszkedtek az előző ACL utasításokra.
- Az eseménynaplózás folyamata további terhelést jelent a forgalomirányító számára.
- A napló tartalma átküldhető egy külső syslog kiszolgálóra.
- A naplózáshoz engedélyezni kell az időbélyeg szolgáltatást, valamint meg kell bizonyosodni arról, hogy a forgalomirányítón a dátum és az idő pontosan be van állítva. Így a naplófájlok mindig a megfelelő időbélyeget jelenítik meg.



9. Hibaelhárítás egy vállalati hálózaton

9.1 A hálózati meghibásodások hatásai

9.1.1 Elvárások a vállalati hálózatokkal szemben

A vállalatok többsége saját hálózataira támaszkodva próbál folyamatos és megbízható hozzáférést biztosítani a megosztott erőforrásokhoz. Hálózati üzemidőnek azt az időtartamot nevezzük, amikor a hálózat rendelkezésre áll és az elvárásoknak megfelelően üzemel. Hálózati leállásnak nevezünk minden olyan időszakot, amikor a hálózat nem a kívánalmak szerint teljesít. A hálózat teljesítményének csökkenése negatívan befolyásolhatja az üzletvitelt.

Megbízható hálózat hiányában számos szervezet veszítheti el hozzáférését az ügyféladatokat tartalmazó adatbázisokhoz és a számviteli nyilvántartásokhoz, holott erre az alkalmazottaknak szükségük van mindennapi munkájuk során. Ezen felül a hálózati leállások megakadályozzák az ügyfeleket rendeléseik feladásában vagy az általuk igényelt információk megszerzésében. A leállás termeléskiesést és az ügyfelek csalódottságát eredményezi, valamint gyakran jár azzal, hogy az ügyfelek a konkurenciát választják inkább.

Egy leállás miatt a vállalatnál jelentkező veszteség meghatározására több különböző mérési módszert használnak. Egy adott vállalat számára a tényleges költség a napszak, a dátum és az időpont függvényében változik.

A nagyvállalatok többnyire több időzónában is rendelkeznek telephellyel, alkalmazottaik, ügyfeleik és beszállítók pedig a nap minden szakában használják a vállalati hálózatot. Az ilyen szervezetek esetében rendkívül költséges bármilyen leállás. Számos tényező okozhat hálózati leállást. Ilyenek például az alábbiak:

- Időjárási és természeti katasztrófák
- Betörések
- Emberi beavatkozás által előidézett katasztrófák
- Túlfeszültség lökések
- Vírustámadások
- Meghibásodott berendezések
- Rosszul konfigurált eszközök
- Erőforráshiány

Egy jól elkészített hálózati terv és annak megvalósítása kritikus fontosságú ahhoz, hogy az üzemidő az elvárások szerint alakuljon.

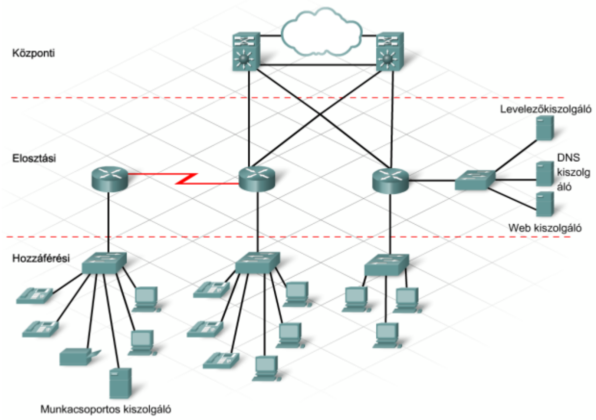
Egy jól megtervezett hálózat a megfelelő és hatékony adatáramlás biztosításához redundánsan tartalmaz minden kritikus fontosságú összetevőt és adatútvonalat. Ez a redundancia kizárja az egyetlen pontból eredő meghibásodásokat.

A háromrétegű hierarchikus hálózattervezési modell funkcionálisan választja szét egymástól a különféle hálózati eszközöket és összeköttetéseket. Ez az elkülönítés gondoskodik a hálózat

teljesítményének hatékonyságáról. A fenti hálózattervezési modell és a vállalati kategóriába tartozó eszközök együttes alkalmazása nagymértékű megbízhatóságot eredményez.

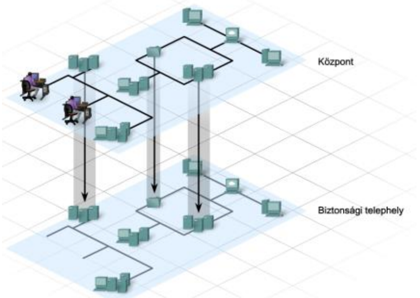
Még a megfelelő hálózati terv megléte esetén is elkerülhetetlen lehet esetenkénti leállás a hálózatban. A leállási idő minimalizálásához és a gyors helyreállás biztosításához további tényezőket kell figyelembe venni.

A szolgáltatási szintek garantálásához, a vállalatnak és a fő szolgáltatóknak szolgáltatói szerződésekben (SLA) kell megegyezniük egymással. Egy SLA világosan rögzíti a szolgáltatás szintjével szemben támasztott elvárásokat. Ezen elvárások közé tartozik például az elfogadható mértékű hálózati leállás és a helyreállítás időtartama is. Ezekben a szerződésekben gyakran előírják a szolgáltatás bármely hiányosságához társított jóvátétel mértékét is.



Leállások nem csak az ISP-k szolgáltatásainak hiányosságai miatt következhetnek be. Elég gyakran a probléma a helyi hálózat részét képező kulcsfontosságú eszköz meghibásodásából ered. Az ilyen típusú leállások előfordulásának minimalizálásához jótállásra van szükség az összes kritikus fontosságú berendezésre nézve. A jótállás gondoskodik a létfontosságú összetevők gyors cseréjéről.

Az üzletfolytonossági tervek részletes akciótervvel szolgálnak az olyan nem várt, mesterségesen előidézett vagy természeti katasztrófák esetén, mint például az áramkimaradások vagy a földrengések. Az üzletfolytonossági tervek részletezik azt, hogy miként folytatódjanak vagy induljanak újra a vállalat tevékenységei a katasztrófa után úgy, hogy az ügyfeleket ez a lehető legkisebb mértékben zavarja csak. Egyértelműen leírják, hogyan fog a hálózat működőképessége újra kialakulni egy kritikus meghibásodás esetén. A működőképesség biztosításának egyik módja, ha egy redundáns, biztonsági telephellyel rendelkezünk egy másik helyszínen, arra az esetre, ha az elsődleges telephely meghibásodna.



9.1.2 Nyomon követés és megelőző karbantartás

A hálózati üzemidő biztosításának egyik módja a hálózati működés folyamatos nyomon követése és a megelőző karbantartási feladatok elvégzése.

A hálózat megfigyelésének célja az, hogy a hálózat teljesítménye összevethető legyen egy előre meghatározott viszonyítási alapértékkel. Bármilyen észlelt eltérés ettől a viszonyítási alaptól a hálózat egy lehetséges hibájáról árulkodik és kivizsgálást igényel. Amint a hálózati rendszergazda meghatározza a teljesítmény csökkenésének okát, elvégezhető a helyreállítás, s így elkerülhető a komolyabb hálózati üzemszünet.

Számos eszközcsoport áll rendelkezésre a hálózati teljesítményszintek nyomon követéséhez és adatok gyűjtéséhez. Ilyen eszközök például az alábbiak:

- Hálózati segédprogramok
- Csomagvizsgáló (packet sniffing) eszközök
- SNMP felügyeleti eszközök

Az egyes eszközcsoportok különböző lehetőségekkel rendelkeznek és különböző típusú információkat szolgáltatnak. Az ilyen eszközök kombinált használatával átfogó képet kaphatunk a hálózat pillanatnyi teljesítményéről.

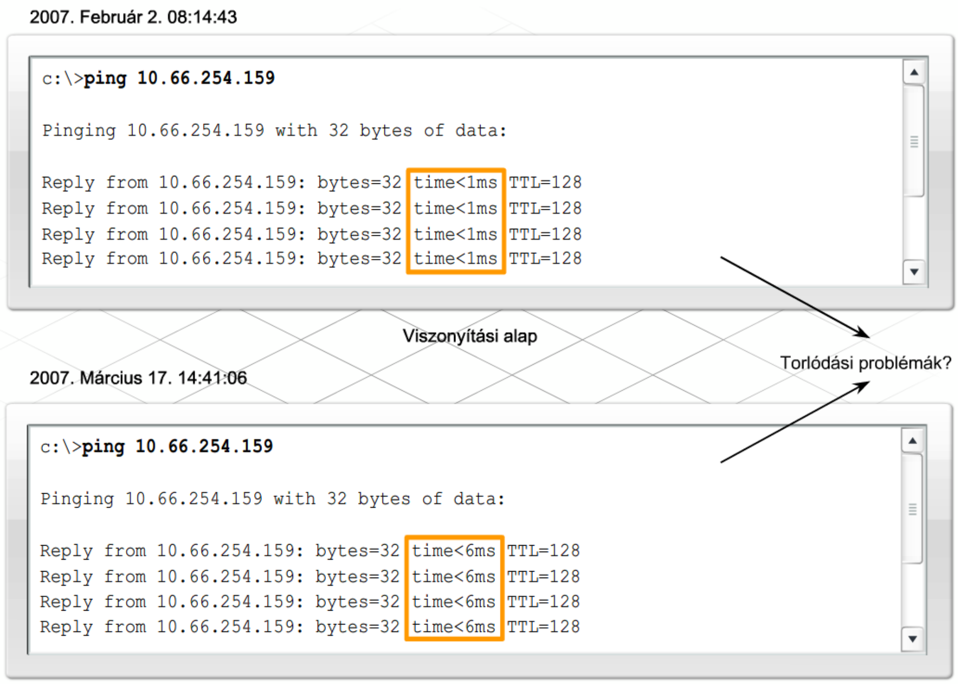
Egy hálózati rendszergazda rendszeresen proaktív (megelőző) karbantartási feladatokat végez a berendezések ellenőrzéséhez és karbantartásához. Ezzel a rendszergazda még egy kritikus hiba bekövetkezése előtt képes lehet megtalálni azokat a gyenge pontokat, amelyek a hálózat leállását okozhatnák. Csakúgy, mint egy autó rendszeres szervízelése esetén, a proaktív karbantartás meghosszabbítja a hálózati eszköz élettartamát.

A hálózatfigyelő eszközök, módszerek és programok használatához szükség van egy teljes körű, pontos és aktuális hálózati dokumentációra. Az ilyen dokumentációknak a következőket kell tartalmazniuk:

- Fizikai és logikai topológia diagramok
- Minden hálózati eszköz konfigurációs állománya
- Viszonyítási teljesítményszint

Bevált gyakorlatnak számít a hálózat első telepítése után, illetve minden nagyobb változtatást vagy fejlesztést követően meghatározni a viszonyítási teljesítményszinteket. A hálózati rendszergazdák normális terheltségi szintek mellett végzik a hálózat tesztelését, olyan protokollok és alkalmazások használatával, melyek általánosan előfordulnak a hálózaton.

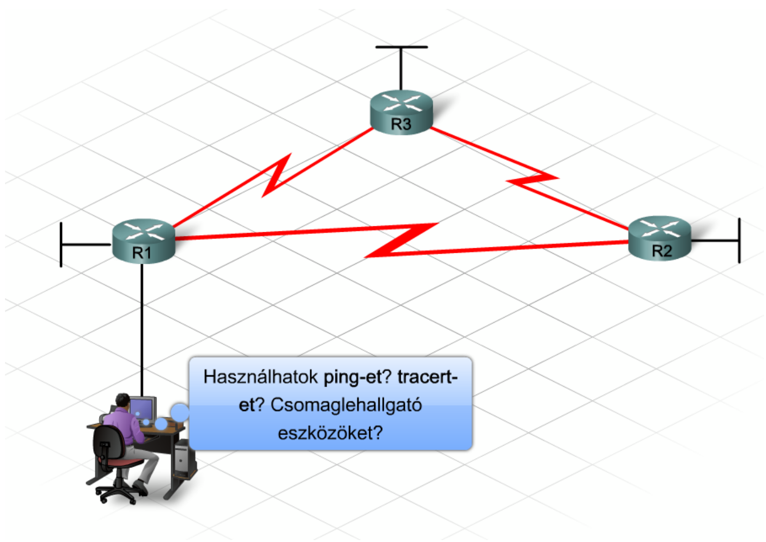
Számos összetett eszköz és eljárás létezik a viszonyítási teljesítményszintek megállapításához. Néhány program több különböző tesztet végez el, különböző típusú hálózati forgalmakat használva. A tesztek nagyon pontosan meghatározott terhelési állapotok és feltételek mellett állapítják meg a hálózat teljesítményét. Más eszközök, mint például a ping, jóval pontatlanabbak, viszont gyakran elegendő információt szolgáltatnak ahhoz, hogy figyelmeztessék a rendszergazdát egy problémára.



Az egyszerű hálózati segédprogramok, mint a ping vagy a tracert, információt szolgáltatnak a hálózat vagy a hálózati kapcsolat teljesítményéről. Ezen parancsok többszöri alkalmazásával megjeleníthető egy csomag két hely közötti átvitelének időbeli eltérése. Mindemellett ezeknek a parancsoknak a használata nem ad magyarázatot az időkülönbségekre.

A csomagvizsgáló eszközök figyelemmel kísérik a forgalomtípusokat a hálózat különböző részein. Ezek az eszközök jelzik, ha egy bizonyos forgalomtípus rendkívül nagy mennyiségben van jelen. A csomagok tartalmát megvizsgálva képesek pillanatok alatt meghatározni az érintett forgalom forrását.

Ezek az eszközök esetenként képesek a problémát orvosolni is, még mielőtt a hálózat túlterheltsége kritikussá válna. Például forgalomlehallgatás segítségével felismerhetőek a hálózatban előforduló nemkívánatos forgalomtípusok és műveletek. Ez a felismerés megállíthat egy lehetséges szolgáltatás megtagadásos (DoS) támadást, mielőtt az befolyásolná a hálózat teljesítményét.

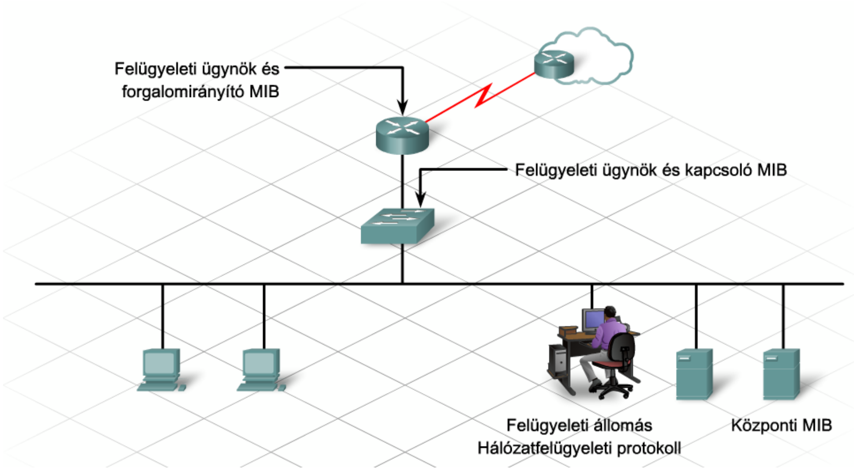


Az egyszerű hálózatfelügyeleti protokoll (SNMP) lehetővé teszi egyedi berendezések megfigyelését a hálózaton. Az SNMP-képes eszközök beépitett SNMP ügynökprogramokat használnak néhány előre meghatározott paraméter bizonyos körülmények között történő megfigyeléséhez. Ezek az ügynökök összegyűjtik az információkat és egy saját, felügyeleti információs adatbázis (MIB) néven ismert adatbázisban tárolják azokat.

Az SNMP szabályos időközönként lekérdezéssel begyűjti az az eszközöktől a felügyelt paraméterekre vonatkozó információkat. Ezenfelül az SNMP képes olyan események detektálására, amelyek túllépnek egy előre meghatározott küszöbértéket vagy feltételt.

Az SNMP például megfigyelheti egy forgalomirányító interfészének hibáit. A hálózati rendszergazda ehhez az interfészhez meghatározza a hibák számára vonatkozó még elfogadható szintet. Ha a hibák száma túllépi a küszöbértéket, az SNMP észleli ezt az állapotot, és elküldi azt a hálózatfelügyeleti állomásnak (NMS). Az NMS riasztja a hálózati rendszergazdát. Némely SNMP rendszer olyan eseményeket vált ki a probléma kiküszöböléséhez, mint például egy eszköz automatikus újrakonfigurálása. A legtöbb vállalati szintű hálózatfelügyeleti rendszer SNMP-t használ.

Sok ingyenes (freeware) és kereskedelmi verziójú proaktív hálózatfigyelő eszköz létezik. Ezekkel az eszközökkel megfigyelhető a forgalom típusa és terhelése, a kiszolgálók konfigurációja, forgalom-minták és számos egyéb körülmény. Egy jó hálózat-megfigyelési terv és a megfelelő eszközök használata segítségére lehet a hálózati rendszergazdának a hálózat állapotának kiértékelésében és a problémás szituációk észlelésében.



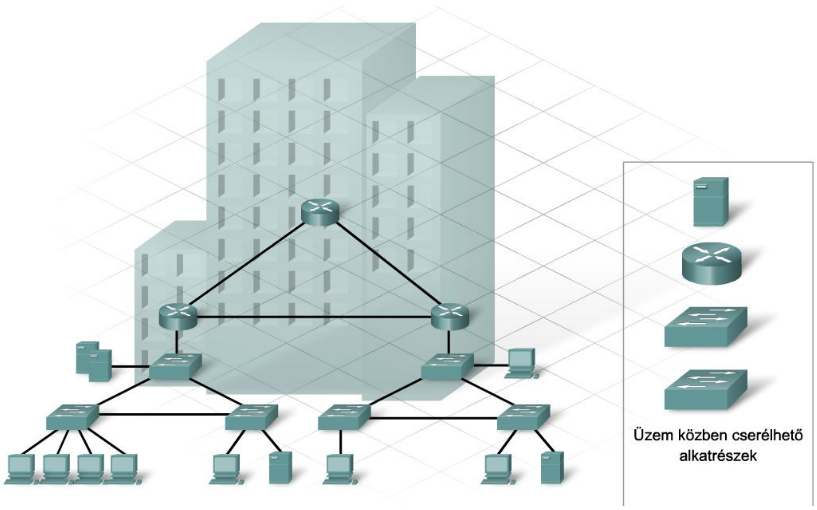
9.1.3 Hibaelhárítás és hibatartomány

Minden hibaelhárítási törekvésnek az a célja, hogy gyorsan visszaálljon a működőképes állapot, és mindez a végfelhasználókat minél kevésbé érintse. E cél elérése gyakran azzal jár, hogy a működőképesség gyors helyreállításának érdekében el kell halasztani a probléma okának meghatározásához szükséges kiterjedt vagy hosszadalmas folyamatot.

Néhány esetben, egy átmeneti megoldás lehetővé teszi a probléma kivizsgálásának és kijavításának elhalasztását egy későbbi, kevésbé kritikus időszakra.

A redundancia kulcsfontosságú tervezési alkotóelem a vállalati hálózatok esetében. Redundáns környezetben, ha egy összeköttetés leáll, akkor azonnal megindul a forgalom elterelése a tartalék összeköttetés felé. Ez az átmeneti megoldás lehetővé teszi a hálózat működőképességének

fenntartását, és időt ad a rendszergazdának a meghibásodott összeköttetés hibájának megállapításához és kijavításához. Ha egy adott eszközzel vagy konfigurációval probléma adódik, akkor a konfigurációs állományokról készült biztonsági másolat vagy egy tartalék eszköz az összeköttetés gyors helyreállítását teszik lehetővé.



Az ilyen gyors megoldások nem mindig lehetségesek és nem minden esetben nyújtanak kielégítő eredményt. A hálózat és a benne lévő erőforrások biztonságát első számú prioritásként kell kezelni. Ha egy gyors javítás veszélyezteti az előbb említett biztonságot, szánjunk időt egy alkalmasabb, alternatív megoldás felkutatására.

A hálózat biztonsági vonatkozásait az üzletfolytonossági tervben is részletezni kell. A terv a következőket tartalmazza:

- A lehetséges problémák dokumentálása
- A problémák bekövetkezésekor elvégzendő intézkedések leírása
- A vállalat biztonsági házirendjének részletei
- Az intézkedések biztonsági kockázatainak részletei

Vállalati hálózatok tervezése során korlátozni kell a hibatartományok méretét. A hibatartomány a hálózat azon része, amelyre hatással van egy hálózati eszköz meghibásodása vagy hibás konfigurációja. A tartomány tényleges mérete függ az eszköztől és a meghibásodás vagy a konfigurációs hiba típusától. Egy hálózat hibaelhárításakor határozzuk meg a probléma hatókörét és határoljuk körül az érintett hibatartományt.

Ha egy időben hibásodik meg egy 2. rétegbeli kapcsoló és egy határ forgalomirányító is, akkor ezek különböző hibatartományokra vannak hatással.

Egy LAN szegmensen lévő 2. rétegbeli kapcsoló meghibásodása csak a szórási tartományban lévő felhasználókra van hatással, és nincs befolyással a hálózat többi tartományára. Egy határ forgalomirányító meghibásodása azonban meggátolja a vállalat minden felhasználóját a helyi hálózatukon kívül található hálózati erőforrások elérésében.

A forgalomirányítónak nagyobb befolyása van a hálózat működésére nézve, ezért nagyobb hibatartománnyal bír. Normális körülmények mellett a hibaelhárítást először a nagyobb méretű hibatartomány erőforrásaival kell elkezdeni.

Néhány esetben a hibatartomány mérete nem számít döntő tényezőnek a hibaelhárítás során. Ha egy az üzletvitel szempontjából kritikus fontosságú kiszolgáló csatlakozik egy meghibásodott kapcsolóhoz, akkor e probléma kijavítása elsőbbséget élvez a határ forgalomirányítóval szemben.

9.1.4 A hibaelhárítási folyamat

Amikor egy vállalati hálózatban valamilyen probléma következik be, nagyon fontos a probléma gyors és hatékony elhárítása a hosszú ideig tartó leállás elkerülése érdekében. Több strukturált és strukturálatlan problémamegoldó technika áll a hálózati szakemberek rendelkezésére. Ezek közé tartoznak például az alábbiak:

- Fentről lefelé
- Lentről felfelé
- Oszd meg és uralkodj
- Próbálgatás
- Helyettesítés

A legtöbb tapasztalt hálózati szakember a korábban megszerzett tapasztalatokra támaszkodik, és a próbálgatás szemléletével kezdi el a hibaelhárítási folyamatot. A probléma ily módon történő kijavításával sok idő megtakarítható.

Sajnos a kevésbé tapasztalt szakemberek nem hagyatkozhatnak kizárólag a korábban megszerzett tapasztalatokra, és a próbálgatásos megközelítés nem is mindig jár eredménnyel. A fentiek miatt a hibaelhárításhoz egy strukturáltabb megközelítésre van szükség.

Amikor olyan helyzet adódik, amikor strukturáltabb megközelítésre van szükség, a legtöbb hálózati szakember az OSI vagy a TCP/IP modellek rétegein alapuló módszert alkalmaz. A szakember a korábbi tapasztalatait felhasználva meghatározza, hogy a probléma az OSI modell alsóbb vagy felsőbb rétegeivel kapcsolatos-e. A réteg szabja meg, hogy a fentről lefelé vagy a lentről felfelé történő megközelítés lesz-e a megfelelő.

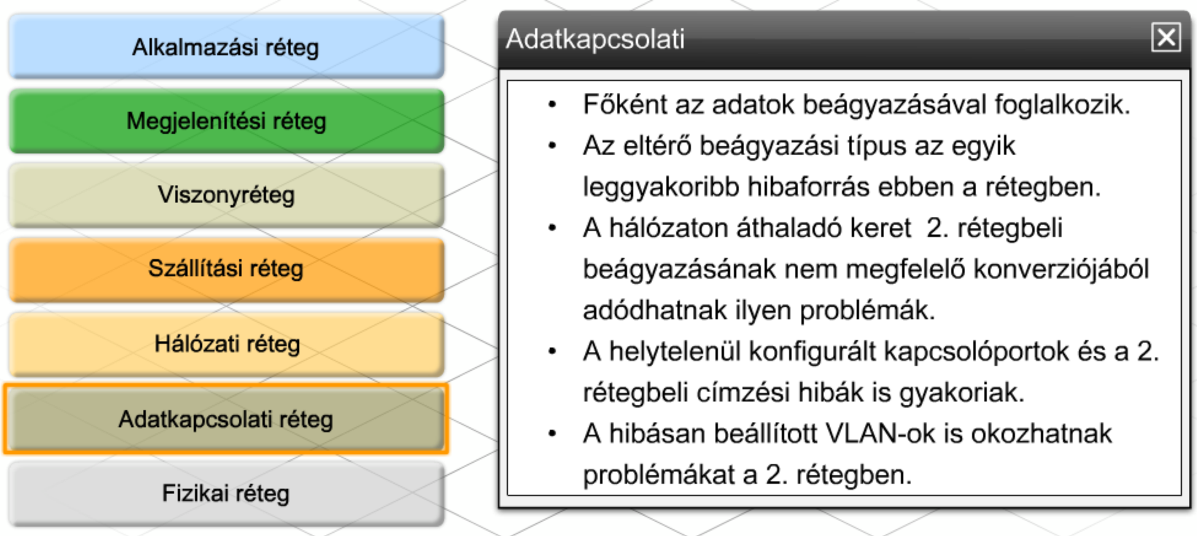
Egy problémás szituáció megközelítése során kövessük az általános problémamegoldó modellt, tekintet nélkül az alkalmazott hibaelhárítási technika típusára.

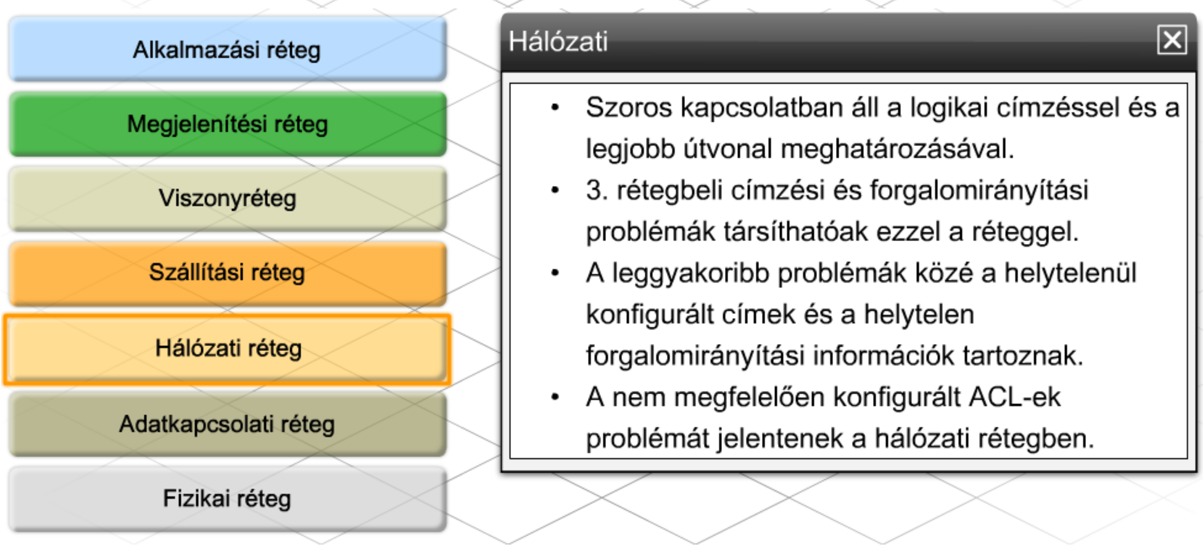
- Határozzuk meg a problémát!
- Gyűjtsük össze a fennálló körülményeket!
- Következtessünk a lehetőségekre és az alternatívákra!
- Hozzunk létre egy intézkedési tervet!
- Valósítsuk meg a megoldást!
- Elemezzük az eredményeket!

Ha ezzel az eljárással első nekifutásra nem tudjuk meghatározni és kijavítani a problémát, akkor szükség szerint ismételjük meg a folyamatot!

Dokumentáljuk a kezdeti tüneteket és minden előfordulást a probléma okának megtalálása és annak kijavítása érdekében! Ez a dokumentáció értékes eszközként szolgálhat egy ilyen vagy ehhez hasonló probléma bekövetkezése esetén. Még a sikertelen próbálkozásokat is fontos dokumentálni, hogy időt takaríthassunk meg a jövőbeni hibaelhárítási tevékenységek során.

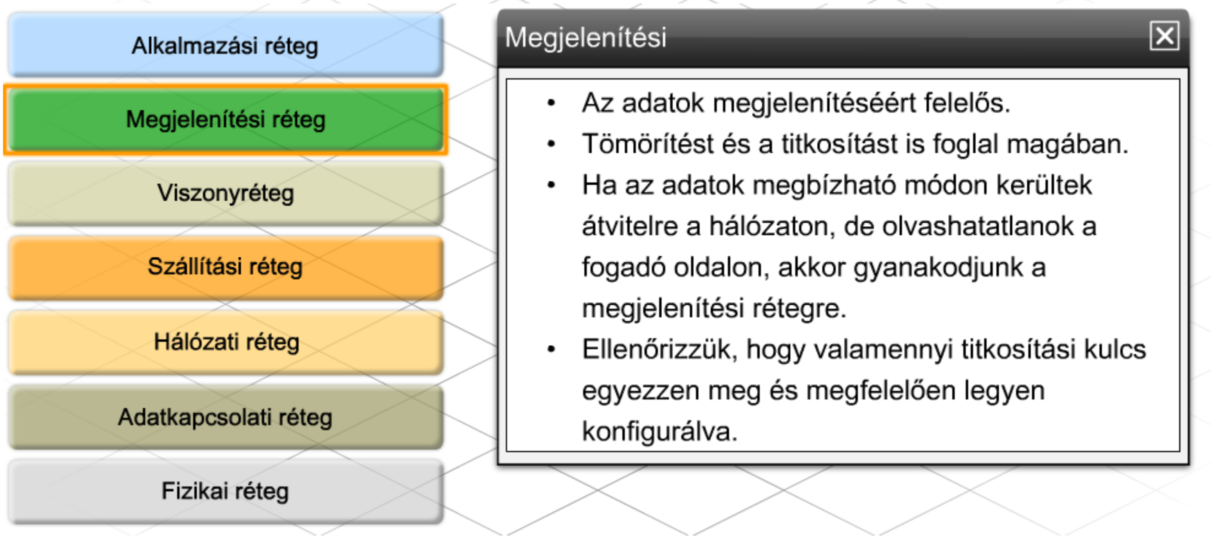


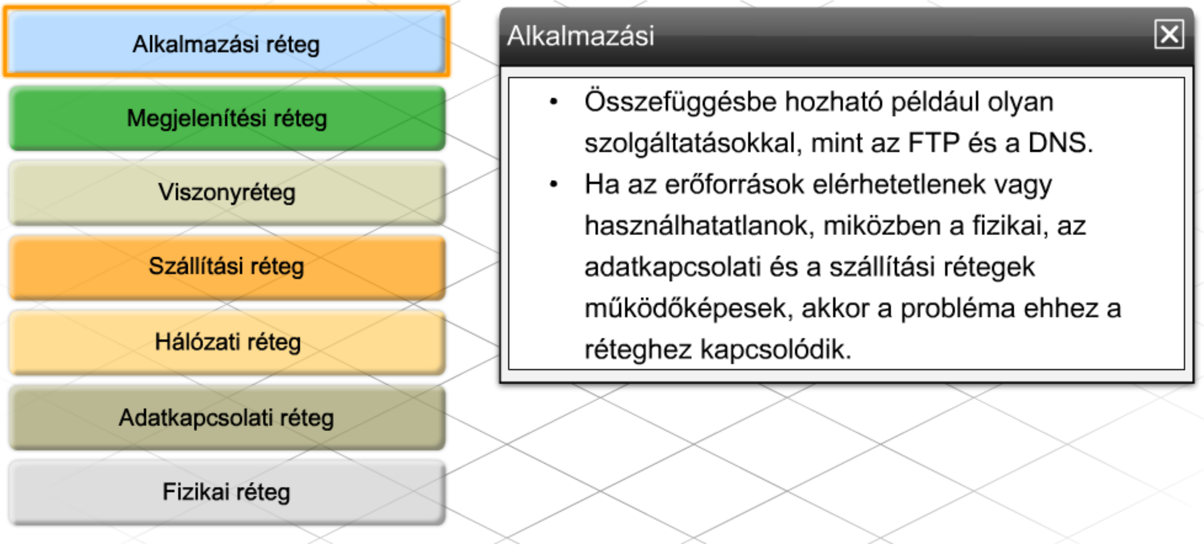





Alkalmazási réteg
Megjelenítési réteg
Viszonyréteg
Szállítási réteg
Hálózati réteg
Adatkapcsolati réteg
Fizikai réteg
Szállítási
• Portszámokat használ a párbeszéd során átvitt forgalomtípusok azonosításához.
• A helytelenül konfigurált ACL-ek gyakran okoznak problémát ebben a rétegben.


Alkalmazási réteg
Megjelenítési réteg
Viszonyréteg
Szállítási réteg
Hálózati réteg
Adatkapcsolati réteg
Fizikai réteg
Viszony
• Az alkalmazások közötti, végponttól-végpontig terjedő kommunikációs folyamatok létrehozásáért, fenntartásáért és befejezéséért felelős.
• A szinkronizációval és az áramlásvezérléssel áll összefüggésben.
• Egy alkalmazáskiszolgáló meghibásodása a kommunikációs folyamat során problémákat okozhat a viszony rétegben.


Alkalmazási réteg
Megjelenítési réteg
Viszonyréteg
Szállítási réteg
Hálózati réteg
Adatkapcsolati réteg
Fizikai réteg
Megjelenítési
• Az adatok megjelenítéséért felelős.
• Tömörítést és a titkosítást is foglal magában.
• Ha az adatok megbízható módon kerültek átvitelre a hálózaton, de olvashatatlanok a fogadó oldalon, akkor gyanakodjunk a megjelenítési rétegre.
• Ellenőrizzük, hogy valamennyi titkosítási kulcs egyezzen meg és megfelelően legyen konfigurálva.



9.2 Kapcsolási és kapcsolódási problémák hibaelhárítása

9.2.1 Kapcsolók alapvető hibaelhárítása

Jelenleg a kapcsolók a leggyakrabban használt hozzáférés rétegbeli hálózati eszközök. A munkaállomások, nyomtatók és kiszolgálók kapcsolókon keresztül csatlakoznak a hálózathoz. A kapcsoló hardveres vagy konfigurációs hibái megakadályozzák a helyi és távoli eszközök között az összeköttetést.

A kapcsolóknál fellépő leggyakoribb hibák a fizikai réteg szintjén következnek be. Ha egy kapcsolót nem kellően védett környezetbe telepítettek, akkor olyan károsodásokat is elszenvedhetnek, mint a kimozdult vagy megsérült adat- és tápkábelek. Győződjünk meg róla, hogy a kapcsolókat fizikailag védett területen helyezték el!

Ha egy végponti eszköz nem képes csatlakozni a hálózathoz és a kapcsolatjelző LED nem világít, akkor az összeköttetés vagy a kapcsolóport hibásodott meg, vagy állt le. Ebben az esetben végezzük el az alábbi lépéseket:

- Győződjünk meg róla, hogy világít-e az áramellátást jelző LED!
- Győződjünk meg arról, hogy a megfelelő típusú kábel csatlakoztatja-e a végponti eszközt a kapcsolóhoz!
- Húzzuk ki és dugjuk be újra a kábeleket a munkaállomásnál és a kapcsolónál is!
- Ellenőrizzük a konfigurációt annak érdekében, hogy a port ne letiltott állapotban legyen!

Ha kapcsolódási probléma áll fenn és világít a kapcsolatjelző LED, akkor valószínűleg a kapcsoló konfigurációja okozza a problémát.

Abban az esetben, ha egy kapcsolóport nem megfelelően vagy hibásan működik, a legegyszerűbb tesztelési módszer az, ha egy másik portba csatlakoztatjuk a hálózati kábelt, és ellenőrizzük, hogy ez megoldotta-e a problémát.

Győződjünk meg arról, hogy nem tiltotta-e le a portot a kapcsoló portvédelme. Ez az alábbi parancsok segítségével ellenőrizhető:

```
show running-config
```

```
show port-security interface interface_azonosító
```

Ha a kapcsoló védelmi beállításai tiltották le a portot, akkor ellenőrízzük le a biztonsági házirendben, hogy megengedett-e a biztonsági szabályok megváltoztatása.

A kapcsolók a 2. rétegben működnek, és egy táblában nyilvántartást vezetnek minden csatlakoztatott eszköz MAC-címéről. Ha ebben a táblában egy MAC-címhez helytelen bejegyzés tartozik, akkor a kapcsoló nem a megfelelő port felé fogja továbbítani az információt, és így a kommunikáció nem jön létre.

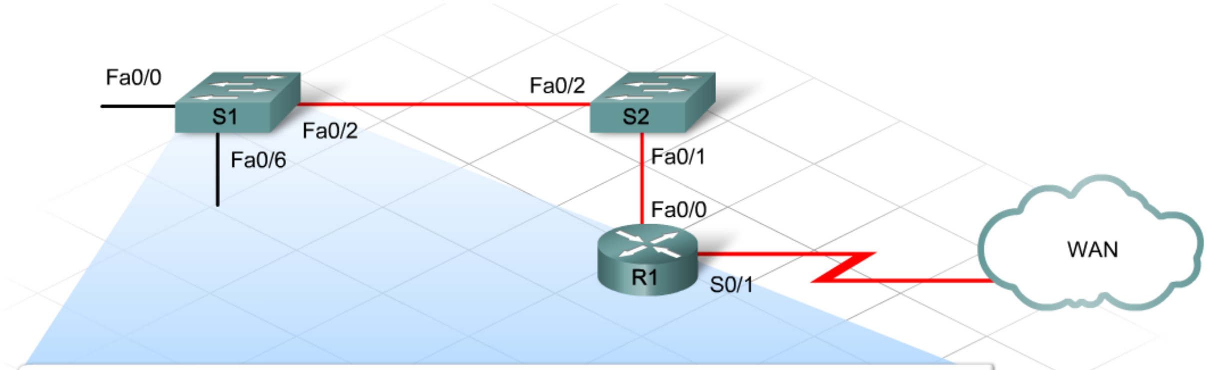
Az egyes kapcsolóportokhoz csatlakoztatott eszközök MAC-címeinek megtekintéséhez a következő parancs használható:

```
show mac-address-table
```

A tábla dinamikus bejegyzéseinek törléséhez adja ki az alábbi parancsot:

```
clear mac-address-table dynamic
```

A kapcsoló ezt követően a legfrissebb információk alapján újra feltölti MAC-cím táblát.




```
S1#show mac-address-table
Mac Address Table
-------------------------------------------------------------------

Vlan   Mac Address                      Type           Ports
----   -----------                      -----          ------
All    000.d.6563.bd00                  STATIC         CPU
All    0100.0ccc.cccc                   STATIC         CPU
All    0100.0ccc.cccd                   STATIC         CPU
All    0100.0cdd.dddd                   STATIC         CPU
  1    000d.29a0.88e0                   DYNAMIC        Fa0/2
  1    000d.6563.0582                   DYNAMIC        Fa0/2
  1    0010.a4fa.b23e                   DYNAMIC        Fa0/6
```

```
  1    00b0.d04d.01f7                   DYNAMIC        Fa0/4
101    000d.29a0.88e0                   DYNAMIC        Fa0/2
101    000d.6563.0582                   DYNAMIC        Fa0/2
102    000d.29a0.88e0                   DYNAMIC        Fa0/2
102    000d.6563.0582                   DYNAMIC        Fa0/2
103    000d.29a0.88e0                   DYNAMIC        Fa0/2
103    000d.6563.0582                   DYNAMIC        Fa0/2
Total Mac Addresses for this criterion: 14
```

Annak ellenére, hogy számos eszköz képes a sebesség és a duplexitás automatikusan észlelésére, az erre vonatkozó egymással nem egyező beállítások meggátolják a kapcsoló és a végponti eszköz közötti összeköttetés működését. Néhány kapcsoló nem megfelelően észleli a csatlakoztatott eszköz sebességét és duplexitását. Amennyiben ez a feltételezett probléma, rögzítsük le az értékeket a kapcsolón a gazdagépnek megfelelően, az interface speed és a duplex parancsok segítségével!

Egy adott port sebességének és duplex beállításainak megjelenítéséhez ez a parancs használható:

```
show interface interface_azonosító
```

A kapcsolódási problémák további lehetséges forrásait a kapcsolási hurkok alkotják. Egy kapcsolt hálózatban az STP elhárítja a kapcsolási hurkokat és a szórási viharokat azáltal, hogy leállítja a redundáns útvonalakat. Ha az STP pontatlan információk alapján hozza meg a döntéseit, hurkok alakulhatnak ki.

Ha hurok van jelen egy hálózatban, annak az alábbi jelei lehetnek:

- Megszűnt az összeköttetés az érintett hálózati tartományok felé, felől és azokon keresztül
- Magas CPU kihasználtság az érintett szegmensekhez csatlakozó forgalomirányítókon
- Az összeköttetés magas, akár 100%-os kihasználtsága
- Magas a kapcsoló ún. hátlapi kommunikációs rendszerének kihasználtsága a viszonyítási pont kihasználtság értékéhez képest
- A syslog üzenetek csomaghurkot vagy állandó cím újratanulást jeleznek, esetleg egy MAC-cím több porton történő észleléséről (MAC address flapping) érkezik figyelmeztető üzenet
- Növekvő számú eldobott kimenő keret több interfészen

Hurok akkor alakul ki, amikor a kapcsoló nem kap BPDU-kat vagy nem képes feldolgozni azokat. Ez a probléma a következők miatt lehet:

- Hibás konfigurációk
- Meghibásodott média konverterek
- Hardveres vagy kábelezési problémák
- Túlterhelt processzorok

A túlterhelt processzorok miatt leállhat az STP működése, és a kapcsolók nem lesznek képesek feldolgozni a BPDU-kat. A több porton is megjelenő MAC-címek megsokszorozzák az átvitelek számát. A megnövekedett átvitelszám túlterhelheti a processzort. Ilyen helyzet csak nagyon ritkán következhet be egy megfelelően konfigurált hálózatban. A problématípus orvoslásához meg kell szüntetni az összes redundáns útvonalat.

Egy másik hibaelhárítási probléma az úgynevezett nem optimális kapcsolás (suboptimal switching) esete. Az alapértelmezett értékeken hagyva az STP nem mindig a legjobb pozicióiú hidat vagy portot választja ki gyökérponti hidnak illetve gyökér portnak. Egy kapcsolón a prioritás értékének megváltoztatásával kényszeríthető ki a megfelelő gyökérponti híd kiválasztása. Az optimális kapcsolás érdekében a gyökérponti hídnak a hálózat központi helyén kell elhelyezkednie.

STP hibaelhárításakor használjuk a következő parancsokat:

Információt ad az STP konfigurációjáról:

```
show spanning-tree
```

Információt ad egy adott interfész STP állapotáról:

```
show spanning-tree interface interface_azonosító
```

9.2.2 VLAN konfigurációs problémák hibaelhárítása

Ha a fizikai réteg rendben működik, és még sincs kommunikáció az eszközök között, ellenőrizzük a VLAN konfigurációt!

Ha a nem működő portok közös VLAN-ba tartoznak, akkor az állomásoknak ugyanazon hálózatba vagy alhálózatba tartozó IP-címmel kell rendelkezniük a kommunikáció érdekében. Ha a nem működő portok különböző VLAN-ba tartoznak, a kommunikáció csak egy 3. rétegbeli eszköz, például forgalomirányító segítségével lehetséges. Ha információra van szükségünk egy bizonyos VLAN-ról, használjuk a `show vlan id vlan_szám` parancsot, amivel megtekinthetőek az egyes VLAN-okhoz rendelt portok!

Ha VLAN-ok közötti forgalomirányítása van szükség, ellenőrizzük a következő konfigurációkat:

- VLAN-onként egy port egy forgalomirányító interfészéhez vagy alinterfészéhez csatlakozzon.
- Mind a kapcsolóport, mind a forgalomirányító interfésze konfigurálva legyen trönkölésre.
- Mind a kapcsolóport, mind a forgalomirányító interfésze ugyanazon beágyazással legyen konfigurálva.

Az újabb kapcsolók alapértelmezés szerinti beállítása a 802.1Q, de néhány Cisco kapcsoló támogatja a 802.1Q-t és a Cisco tulajdonában lévő Inter-Switch Link (ISL) formátumot is. Ahol lehetséges az IEEE 802.1Q-t kell használni, mivel ez számít de facto szabványnak, továbbá a 802.1Q és az ISL nem kompatibilisek egymással.

VLAN-ok közötti forgalomirányítási problémák hibaelhárításakor győződjünk meg arról, hogy a forgalomirányító fizikai interfészének ne legyen IP-címe. Ennek az interfésznek aktívnak kell lennie.

Az interfészek konfigurációjának megtekintéséhez a következő parancs használható:

```
show ip interface brief
```

Az egyes VLAN-okhoz rendelt hálózatnak láthatónak kell lennie a forgalomirányító táblában. Ellenkező esetben ellenőrizzük újra az összes fizikai csatlakozást és a trönk konfigurációját az összeköttetés mindkét végén! Ha a forgalomirányító nem közvetlenül csatlakozik egy vagy több VLAN alhálózatához, ellenőrizzük az irányító protokoll konfigurációját annak érdekében, hogy minden VLAN felé legyen útvonal! Használjuk az alábbi parancsot:

```
show ip route
```

Hozzáférési port vagy trönkport

Minden kapcsolóport vagy hozzáférési portként vagy trönkportként üzemel. Néhány kapcsoló modellen más típusú kapcsolóportok is rendelkezésre állnak, és a kapcsoló automatikusan állítja be a portot a megfelelő állapotba. Néhány esetben ajánlatos rögzíteni a port hozzáférési vagy trönk állapotát, így elkerülhetőek az észlelési folyamat során fellépő lehetséges problémák.

Natív és menedzsment VLAN-ok

A kapcsolóportok vagy hozzáférési portként vagy trönkportként üzemelnek. A trönkvonal natív VLAN-jához vannak hozzárendelve a trönkön átküldött címkézetlen keretek. Ha egy eszközön megváltoztattuk a natív VLAN kiosztást, akkor a 802.1Q trönk mindkét végpontján be kell állítani ugyanazt a natív VLAN azonosítószámot. Ha a trönk egyik végén a VLAN10 lett natívként konfigurálva, a másik végen pedig a VLAN 14, akkor az egyik végen a VLAN10-ből küldött keret a másik oldalon a VLAN14-ben lesz fogadva. Ekkor a VLAN10 „átszivárog” a VLAN14-be. Ez váratlan kapcsolódási problémákat okozhat és növelheti a késleltetést.

A zavartalan, gyors átvitel érdekében ellenőrizzük le, hogy a natív VLAN hozzárendelés ugyanaz legyen minden eszközön az egész hálózatban!

9.2.3 VTP hibaelhárítás

A VTP leegyszerűsíti a VLAN információk szétosztását több kapcsoló között egy tartományon belül. A VTP működésében részt vevő kapcsolók a következő három mód egyikében üzemelnek: kiszolgáló, ügyfél és transzparens. Csak a kiszolgáló veheti fel, törölheti vagy módosíthatja a VLAN információkat.

Amikor VTP hibaelhárítást végzünk egy hálózaton, bizonyosodjunk meg az alábbiakról:

- Minden részt vevő eszköznek ugyanazzal a VTP tartománynévvel kell rendelkeznie.
- Két VTP kiszolgálónak kell lennie minden tartományban arra az esetre, ha az egyik meghibásodna.
- Minden kiszolgálónak ugyanazokkal az információkkal kell rendelkeznie.
- Minden eszköznek ugyanazt a VTP-protokoll verziót kell használnia.

Egy eszközön a használatban lévő VTP-protokoll verzió, a VTP tartománynév, a VTP mód és a VTP-verziószám (revision number) megjelenítéséhez, adjuk ki az alábbi parancsot:

```
show vtp status
```

A VTP-protokoll verzió megváltoztatásához:

```
vtp version <1 | 2>
```

A VTP ügyfelek és kiszolgálók a VTP frissítési-verziószámot használják annak eldöntéséhez, hogy frissíteniük kell-e a VLAN információikat. Ha a frissítés verziószáma magasabb, mint a jelenleg használt verziószám, az ügyfelek és a kiszolgálók felhasználják az újonnan érkezett információkat a konfiguráció frissítéséhez.

Mindig ellenőrizzük le a VTP-verziószámot és a VTP módot, mielőtt bármilyen kapcsolót csatlakoztatnánk a hálózathoz. A verziószámot az NVRAM-ban tárolják a kapcsolók, és az indító konfiguráció törlése nem állítja alaphelyzetbe ezt az értéket. A verziószám alaphelyzetbe hozásához vagy állítsuk a kapcsoló VTP módját transzparensre vagy változtassuk meg a VTP tartománynevet.

Az is problémát okozhat, ha egy illegális illegális (rogue) kapcsoló csatlakozik a tartományhoz, és megváltoztatja a VLAN információkat. Ennek megakadályozásához érdemes jelszót beállítani a VTP

tartományhoz. A tartomány VTP jelszavának beállításához használjuk a következő globális konfigurációs parancsot:

```
vtp password jelszó
```

Ha használunk hitelesítési jelszót, akkor a VTP tartományon belül minden eszközön ugyanazt kell beállítani. Ha a frissítések nem terjednek tovább egy új kapcsoló felé a VTP tartományban, akkor valószínűleg a jelszóval van a probléma. A jelszó ellenőrzéséhez használjuk ezt a parancsot:

```
show vtp password
```

9.3 Forgalomirányítási problémák hibaelhárítása

9.3.1 RIP forgalomirányítási problémák

Számos eszköz létezik a forgalomirányítási problémák elhárításához. . Ezek közé tartoznak az IOS show parancsok, a `debug` parancsok és az olyan TCP/IP segédprogramok, mint a `ping`, a `traceroute` és a `telnet`.

A show parancsok egy pillanatfelvételt jelenítenek meg a konfigurációra vagy egy adott részegységre vonatkozóan. A debug parancsok dinamikus működésűek és valós-idejű információkat szolgáltatnak a forgalom változásáról és a protokollok közötti információcseréről. A TCP/IP segédprogramokat, például a `ping`-et, a kapcsolódás ellenőrzésére használhatjuk.

A show parancsok fontos eszközként szolgálnak például egy forgalomirányító állapotának megismeréséhez, a szomszédos forgalomirányítók észleléséhez, a hálózatban található problémák azonosításához és a hálózat általános megfigyeléséhez. A show és a debug parancsok kombinációját a RIP forgalomirányító protokoll működése közben fellépő hibák elhárításához is használhatjuk.

Mielőtt használnánk a `debug` parancsot, közelítsünk a problémához a lehetséges okokra történő szűkítéssel. A `debug` parancsokat a problémák azonosításához használjuk, ne pedig a hálózati normális működésének megfigyeléséhez!

A RIP egy meglehetősen alapszintű és egyszerűen konfigurálható protokoll. Ennek ellenére felléphet néhány tipikus probléma a forgalomirányítók RIP konfigurálása során.

Kompatibilitási problémák léteznek a RIPv1 és a RIPv2 között. Ha a RIP útvonalakat nem hirdetik a forgalomirányítók, akkor vizsgáljuk meg a következő lehetséges problémákat:

- vagy 2. rétegbeli kapcsolódási problémák
- Szükség van a VLSM alhálózatok kezelésére, de RIPv1 van használatban
- Nem illeszkednek egymással a RIPv1 és a RIPv2 forgalomirányítási konfigurációk
- Hiányoznak vagy helytelenek a network parancsok
- Az interfészek IP-címzése nem megfelelő
- A kimenő interfész lekapcsolt állapotban van
- A hirdetett hálózathoz tartozó interfész lekapcsolt állapotban van
- Helytelenül konfigurált passzív interfészek

A `show ip route` paranccsal történő tesztelés előtt érdemes törölni az irányítótábla tartalmát a `clear ip route *` paranccsal.

Az itt felismert problémákon felül, nagyon fontos, hogy mindig emlékezzünk arra, hogy a RIP mértéke az ugrásszám, mely 15 ugrásra van korlátozva! Ez a korlátozás önmagában is okozhat problémát egy nagyobb vállalati hálózatban.

9.3.2 EIGRP forgalomirányítási problémák

Az EIGRP forgalomirányítási problémák elhárítása során alkalmazott IOS show és debug parancsok közül számos megegyezik a RIP esetén használtakkal. Kizárólag csak az EIGRP hibaelhárításához használható parancsok közé az alábbiak tartoznak:

`show ip eigrp neighbors`

Megjeleníti a szomszédok IP-címeit és az interfészek azonosítóit, amelyeken keresztül megtanulta ezeket a címeket.

`show ip eigrp topology`

Megjeleníti az ismert hálózatok topológia tábláját a legjobb útvonalakkal, az állapotjelzőkkel, a legrövidebb távolsággal és az interfészek azonosítóival együtt.

`show ip eigrp traffic`

Megjeleníti az EIGRP forgalmi statisztikáit a konfigurált autonóm rendszerben, egyebek mellett a küldött és fogadott hello csomagok, valamint a frissítések számát.

`debug eigrp packets`

Valós időben jeleníti meg a szomszédok által egymásnak küldött EIGRP csomagokat.

`debug ip eigrp`

Valós időben jeleníti meg az EIGRP eseményeket, közte az összeköttetések állapotának változásait és a forgalomirányító tábla frissítéseit.

Bizonyos problémák gyakran előfordulnak az EIGRP protokoll konfigurálása során. A következő lehetséges okok miatt nem működhet az EIGRP:

- vagy 2. rétegbeli kapcsolódási problémák
- Hibás címzéssel vagy alhálózati maszkkal rendelkező interfész
- Egymással nem egyező autonómrendszer azonosítók a különböző EIGRP forgalomirányítókon
- Rossz hálózat vagy helytelen helyettesítő maszk van megadva az irányítási folyamatban
- Az összeköttetés leállt vagy torlódás lépett fel
- A kimenő interfész lekapcsolt állapotban van
- Egy hirdetett hálózathoz tartozó interfész lekapcsolt állapotban van

Ha az automatikus útvonalösszegzés engedélyezve van a forgalomirányítókon, miközben az alhálózatok nem összefüggőek, elképzelhető, hogy az útvonalak nem megfelelően lesznek hirdetve.

9.3.3 OSPF forgalomirányítási problémák

Az OSPF kapcsán felmerülő problémák túlnyomó része a szomszédsági kapcsolatok létrehozásával és a kapcsolatállapot-adatbázisok szinkronizálásával függ össze.

Az OSPF kapcsán felmerülő problémák elhárítása

- A szomszédos forgalomirányítóknak ugyanazon OSPF területhez kell tartozniuk.
- A szomszédos forgalomirányítók interfészeinek egymással kompatibilis IP-címmel és alhálózati maszkkal kell rendelkezniük.
- Az egy területen lévő forgalomirányítókon ugyanazt az OSPF hello intervallumot és „halott” intervallumot kell megadni.
- A forgalomirányítóknak az interfészeknek megfelelő hálózatokat kell hirdetniük az OSPF folyamatban való részvételhez.
- A megfelelő helyettesítő maszkokat kell használni a helyes IP-cím tartományok hirdetéséhez.
- A kommunikáció megvalósulásához a hitelesítést megfelelően kell beállítani a forgalomirányítókon.

A szabványos show és debug parancsokon felül, az alábbi parancsok használata segíthet az OSPF-fel kapcsolatos problémák elhárításában:

- `show ip ospf`
- `show ip ospf neighbor`
- `show ip ospf interface`
- `debug ip ospf events`
- `debug ip ospf packet`

9.3.4 Útvonal elosztási problémák

Egy határ-forgalomirányítón (edge router) beállított statikus útvonal legvégső átjáróként szolgál a hálózaton kívül található IP-címmel rendelkező állomásoknak küldendő csomagok számára.

Jóllehet ez a konfiguráció megoldást nyújt a határ-forgalomirányítók számára, viszont nem biztosít kijáratot a belső hálózatból a többi belső forgalomirányító részére. Az egyik megoldás, ha minden egyes belső forgalomirányítón konfigurálunk egy alapértelmezett útvonalat, amely a következő ugrás (next hop) vagy a határ-forgalomirányító felé mutat. Ez a módszer azonban nem alkalmazható hatékonyan a nagyobb hálózatokban. Jobb megoldásnak számít forgalomirányító protokollok használatával a határ-forgalomirányítóról a többi belső forgalomirányító felé hirdetni az alapértelmezett útvonalat. Ennek megvalósításához minden irányító protokoll, beleértve a RIP-et, az EIGRP-t és az OSPF-et is, biztosít mechanizmust.

Bármely irányító protokollt is használjuk, konfiguráljunk egy alapértelmezett „négynullás” statikus útvonalat a határ-forgalomirányítón.

```
ip route 0.0.0.0 0.0.0.0 S0/0/0
```

Ezután állítsuk be a határ-forgalomirányítót, hogy hirdesse vagy terjessze alapértelmezett útvonalát a többi forgalomirányító felé. RIP és OSPF esetén lépjünk be forgalomirányító konfigurációs módba és

használjuk a `default-information originate` parancsot! Az EIGRP azonnal hirdeti az alapértelmezett útvonalakat, de használható a `redistribute static` parancs is.

Az alapértelmezett útvonalak nem megfelelő hirdetése megakadályozza a belső forgalomirányítókhoz csatlakozó felhasználókat a külső hálózatok elérésében.

9.4 WAN konfigurációs problémák hibaelhárítása

9.4.1 WAN kapcsolódás hibaelhárítása

A WAN interfészek konfigurálása során számos potenciálisan problémával kerülhetünk szembe. Ezen problémák némelyike elkerülhetetlen, ha a hálózati rendszergazda az összeköttetésnek csak az egyik vége felett rendelkezik befolyással, és az ISP kezeli a másik véget. Ebben az esetben a hálózati rendszergazda azokat a konfigurációs információkat használja, melyekkel az ISP látta el a kapcsolódás biztosítása érdekében.

A fizikai réteg szintjén előforduló leggyakoribb problémák az órajel, a kábeltípusok és a kilazult vagy hibás csatlakozók miatt adódnak. A soros vonali összeköttetések egy DCE eszközt csatlakoztatnak egy DTE eszközhöz. Két különböző típusú kábel létezik az eszközök csatlakoztatásához: DTE és DCE. Általában a szolgáltatónál lévő DCE eszköz biztosítja az órajelet.

Szemrevételezéssel vizsgáljunk meg minden kábelt laza csatlakozást vagy hibás csatlakozót keresve! Ha egy kábelt nem lehet megfelelően csatlakoztatni, cseréljük ki azt egy biztosan jól működőre!

A kábel típusának megjelenítéséhez, valamint a DTE, DCE állapot és az órajel felismeréséhez használjuk a következő parancsot:

```
show controllers <soros_port>
```

Ahhoz, hogy egy soros összeköttetés működjön, a kapcsolat mindkét végpontján egyeznie kell a beágyazási típusnak. A Cisco forgalomirányítókon a HDLC az alapértelmezett soros vonali beágyazási típus. Mivel a Cisco HDLC és a nyílt szabványú HDLC nem kompatibilisek egymással, ne használjuk az alapértelmezett Cisco beágyazást egy nem-Cisco gyártmányú eszközhöz való csatlakozás során!

Néhány 2. rétegbeli beágyazási típusnak több változata is van. Például a Cisco forgalomirányítók támogatják mind a Cisco saját Frame Relay formátumát, mind az ipari szabványú IETF formátumot. Ezek a formátumok nem kompatibilisek egymással. A Cisco eszközökön a Cisco Frame Relay formátum az alapértelmezett.

Annak megtekintéséhez, hogy egy soros vonalon milyen beágyazás van használatban, használjuk a következő parancsot:

```
show interfaces <soros_port>
```

3. réteggel kapcsolatos konfigurációs beállítások is megakadályozhatják az adatok mozgását egy soros összeköttetésen. Bár soros összeköttetések esetén nem szükséges IP-címeket beállítani, ha használni szeretnénk azokat, akkor az összeköttetés mindkét végpontjának ugyanazon a hálózaton vagy alhálózaton kell lennie.

Az a folyamat, amely soros vonali címfeloldó protokoll (SLARP) néven ismert, hozzárendel egy címet egy soros összeköttetés egyik végpontjához, feltéve, ha az összeköttetés másik vége már konfigurálva van. Az SLARP feltételezi, hogy minden soros vonal egy különálló IP-alhálózat és a vonal egyik végének állomásazonosítója 1, a másik végének pedig 2. Feltételezve azt, hogy a soros összeköttetés egyik vége már konfigurálva van, az SLARP automatikusan konfigurálja az IP-címet a másik oldalon.

Az alábbi paranccsal megtekinthető a beállított IP-cím egy interfészen, valamint a port és a vonali protokoll állapota:

```
show ip interface brief
```

Mielőtt az összeköttetésen megindulna a 3. rétegbeli információk mozgása, mind az interfésznek, mind a protokollnak működőképes állapotban kell lennie. Ha az interfész lekapcsolt állapotban van, akkor magával az interfésszel van probléma.

Ha az interfész működik, de a vonali protokoll van lekapcsolt állapotban, ellenőrizzük, hogy a megfelelő kábel van-e csatlakoztatva és szilárdan kapcsolódik-e a porthoz! Ha ez a lépés nem javítja ki a problémát, akkor cseréljük ki a kábelt!

Ha egy interfész állapota adminisztratívan letiltott (administratively down), annak legvalószínűbb oka az, hogy nem adtuk ki a no shutdown parancsot az interfészen. Az interfészek le vannak tiltva alapértelmezés szerint.

A PPP folyamat magában foglalja mind az LCP mind az NCP fázisokat. Az LCP létrehozza az összeköttetést és ellenőrzi azt, hogy annak minősége megfelelő-e a 3. rétegbeli protokollok használatához. Az NCP lehetővé teszi a 3. rétegbeli forgalom számára az összeköttetésen való áthaladást. Egy elhagyható hitelesítési szakasz van az LCP és az NCP fázisok között.

Minden egyes fázisnak sikeresen be kell fejeződnie, mielőtt a következő megkezdődne.

PPP összeköttetések hibaelhárításakor ellenőrizzük a következőket:

- Befejeződött-e már az LCP fázis?
- Ha konfigurálva van, akkor sikeres volt-e a hitelesítés?
- Befejeződött-e már az NCP fázis?

A következőkben néhány parancs segítséget nyújt a PPP összeköttetések hibaelhárításakor. Az LCP és NCP fázisok állapotainak megtekintéséhez az alábbi parancs használható:

```
show interface
```

A következő parancs az összeköttetés létrehozásának fázisa alatt átküldött, a PPP konfigurációs beállítások egyeztetésére használt PPP csomagok megtekintéséhez használható:

```
debug ppp negotiation
```

A következő utasítás a PPP csomagok áramlásának valós idejű megtekintéséhez használható:

```
debug ppp packet
```

9.4.2 WAN hitelesítés hibaelhárítása

A PPP számos előnnyel rendelkezik az alapértelmezett HDLC soros vonali beágyazáshoz képest. Ezen tulajdonságok közé tartozik a PAP vagy CHAP használata, a végponti eszközök hitelesítése érdekében. Az elhagyható hitelesítési fázis azután következik be, hogy az LCP létrehozta az összeköttetést, de még azelőtt, hogy az NCP engedélyezné a 3. rétegbeli forgalom megindulását.

Ha az LCP nem tud csatlakozni, akkor az elhagyható konfigurációs beállítások – köztük a hitelesítés – egyeztetése elmarad. Az aktív NCP-k hiánya sikertelen hitelesítésre utal.

PPP hitelesítés hibaelhárításakor határozzuk meg, hogy a hitelesítés okozza-e a problémát. Ehhez vizsgáljuk meg az LCP és az NCP-k állapotait a show interface parancs segítségével!

Ha mind az LCP, mind az NCP-k aktívak, akkor a hitelesítés sikeres volt és a probléma máshol található.

Ha az LCP nem aktív, akkor probléma áll fenn a forrás és a cél közötti fizikai összeköttetéssel.

Ha az LCP aktív, de az NCP-k nem azok, akkor a hitelesítésre kell gyanakodni.

A hitelesítés lehet egyutas, illetve kétutas. A fokozott biztonság érdekében használjunk kétutas vagy kölcsönös hitelesítést! A kétutas hitelesítés megköveteli, hogy mindkét végponti eszköz meggyőződjön a másik eszköz hitelességéről.

Az összeköttetés mindkét végén ellenőrizzük, hogy létezzen egy felhasználói bejegyzés a távoli eszköz részére és megfelelő legyen a jelszó. Ha bizonytalanok vagyunk, távolítsuk el a régi felhasználói bejegyzést meghatározó utasítást, majd hozzuk létre újra! A konfigurációnak az összeköttetés mindkét végén ugyanazt a hitelesítési típust kell tartalmaznia.

A hitelesítéssel kapcsolatos leggyakoribb problémák abból erednek, hogy egyrészt elfelejtenek felhasználói bejegyzést konfigurálni a távoli forgalomirányító számára, vagy hibásan állítják be a felhasználói nevet és a jelszót. Alapértelmezés szerint a felhasználói név a távoli forgalomirányító állomásneve. Mind a felhasználói név, mind a jelszó érzékeny a kis- és nagybetűkre.

Ha PAP hitelesítést szeretnénk használni egy aktuális verziójú IOS rendszeren, aktiváljuk azt az alábbi paranccsal:

```
ppp pap sent-username felhasználói_név password jelszó
```

A hitelesítési folyamat nyomon követése gyors módszert biztosít a hiba meghatározásához. Használjuk a következő parancsot a végberendezések által egymásnak küldött, a hitelesítési folyamattal kapcsolatban álló csomagok megjelenítéséhez:

```
debug ppp authentication
```

9.5 ACL-ekkel kapcsolatos problémák hibaelhárítása

9.5.1 ACL-ekkel kapcsolatos problémák meghatározása

Az ACL-k használata komplexebbé teheti a hálózati problémák hibaelhárítási folyamatát. Emiatt nagyon fontos, hogy ellenőrizzük az alapszintű hálózati összeköttetést, mielőtt alkalmaznának egy ACL-t.

Amikor ACL-eket használnak, és elérhetetlenné válnak hálózatok vagy állomások, lényeges annak meghatározása, hogy az ACL okozza-e a problémát. A következő kérdések segíthetnek a probléma azonosításában:

- Van-e ACL alkalmazva a problémás forgalomirányítóra vagy interfészre?
- Nemrég lett-e alkalmazva?
- Létezett-e a probléma az ACL alkalmazása előtt?
- Az ACL az elvárásoknak megfelelően működik?
- Érinti-e a probléma az interfészhez csatlakozó összes állomást vagy csak bizonyos állomásokat?
- Minden továbbításra kerülő protokollt érint a probléma vagy csak bizonyos protokollokat?
- A hálózatok az elvárásoknak megfelelően jelentek meg a forgalomirányító táblában?

Ezen kérdések közül néhányra választ kaphatunk a naplózás engedélyezésével. A naplózás megmutatja, hogy milyen hatással van az ACL a különböző csomagokra. Alapértelmezés szerint az egyezések száma a `show access-list` paranccsal jeleníthető meg.

Az engedélyezett, illetve tiltott csomagok részleteinek megtekintéséhez tegyük az ACL parancsok végére a `log` kulcsszót.

Számos parancs segíthet annak meghatározásában, hogy megfelelően vannak-e konfigurálva és alkalmazva az ACL-ek.

A forgalomirányítón konfigurált összes ACL megjelenítéséhez, attól függetlenül, hogy alkalmazva lett-e egy interfészre vagy sem, használjuk a következő parancsot:

```
show access-lists
```

Az egyes ACL utasításokhoz tartozó illeszkedési számlálók törléséhez a következő parancs használható:

```
clear access-list counters
```

A forgalomirányító bármely interfésze által fogadott vagy küldött összes csomag forrás és cél IP-címének megjelenítéséhez az alábbi parancs használható:

```
debug ip packet
```

A debug ip packet parancs azokat a csomagokat mutatja meg, melyeknek forrás-, illetve célcíme egy forgalomirányító interfésze. Azok a csomagok is megjelennek a parancs hatására, amelyeket letiltott egy ACL az interfészen. Néhány forgalomtípus, melyek debug üzeneteket hoznak létre:

- RIP frissítések egy forgalomirányító interfésze irányából vagy irányába

- Bármilyen külső forrásból származó, külső célállomás felé tartó telnet forgalom, melyet blokkolt egy ACL az interfészen.

Ha a csomagok egyszerűen továbbhaladnak, és az ACL nem blokkol egyetlen csomagot sem erről az IP-címről, akkor nem keletkeznek debug üzenetek.

9.5.2 ACL konfigurációs és elhelyezési problémák

Egy helytelenül konfigurált ACL-ből olyan problémák is adódhatnak, mint a lelassult vagy elérhetetlené vált hálózatok. Néhány esetben elképzelhető, hogy az ACL engedélyezi vagy tiltja a tervezett hálózati forgalmat, viszont emellett nem várt hatásai lehetnek más forgalomtípusokra. Ha úgy tűnik, hogy az ACL okozza a problémát, akkor számos dolgot kell megvizsgálni.

Amennyiben az ACL utasítások nem a leghatékonyabb sorrendben követik egymást ahhoz, hogy azok a hozzáférési listában minél korábban engedélyezzék a legnagyobb mennyiségű forgalmat, ellenőrizzük a naplózás eredményeit egy hatékonyabb sorrend meghatározásához!

Az implicit deny utasításnak nem várt következményei lehetnek más forgalomtípusokra nézve. Ebben az esetben egy explicit `deny ip any any log` parancs használatával megfigyelhetőek azok a csomagok, melyekre nem történt egyezés egyetlen korábban szereplő ACL utasítás részéről sem.

Használjunk naplózást annak eldöntéséhez, hogy az ACL optimálisan, illetve az elvártak szerint működik-e!

Annak meghatározásán túl, hogy az ACL megfelelően lett-e konfigurálva, az is nagyon fontos, hogy az ACL a helyes forgalomirányító interfészre legyen alkalmazva és a megfelelő irányban. Egy helyesen konfigurált, de nem megfelelően alkalmazott ACL, az ACL-ek létrehozása során előforduló egyik leggyakoribb probléma.

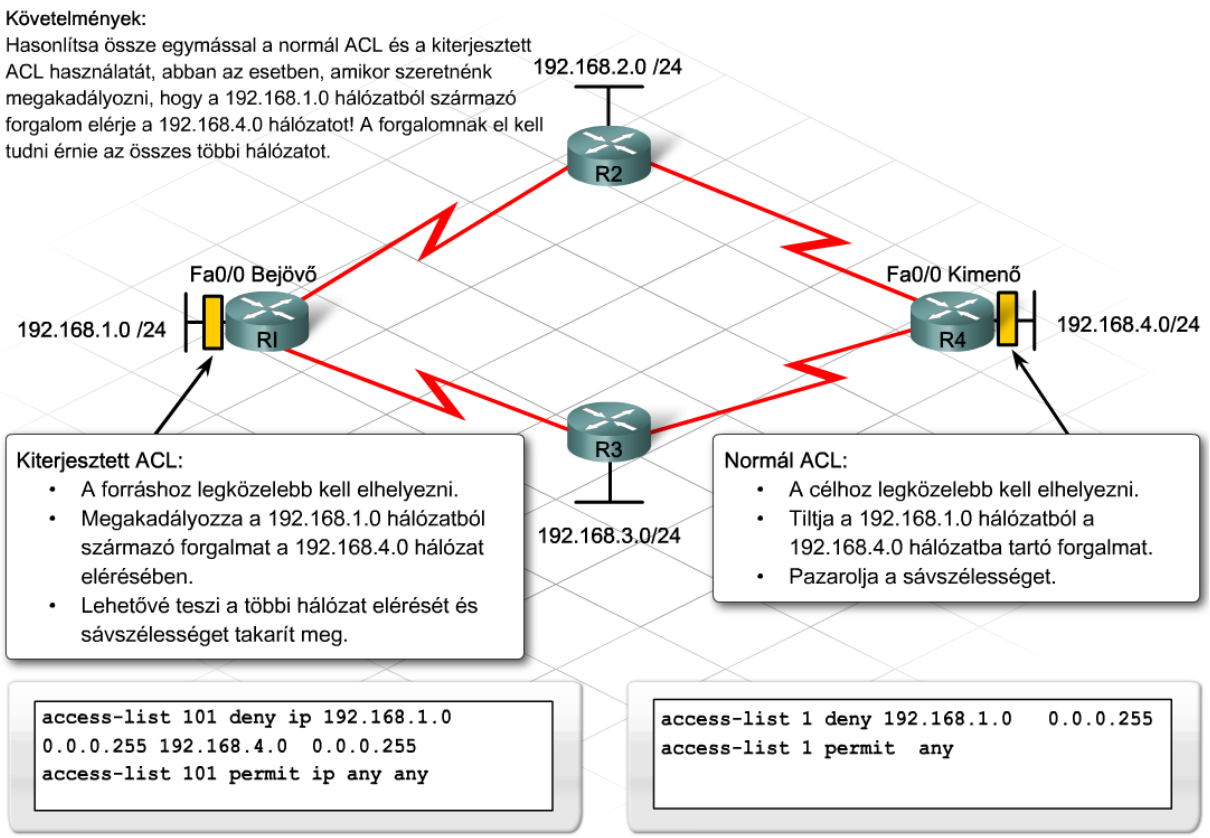
A normál ACL-ek csupán a forrás IP-címet szűrik, ezért lehetőleg a célhoz legközelebb kell elhelyezni azokat.

Egy a forráshoz közel elhelyezett normál ACL olyan hálózati forgalmakat is blokkolhat, amelyeket egyébként át kellene engednie.

A célhoz közel elhelyezett ACL sajnos egy vagy több hálózati szegmensen át lehetővé teszi a forgalom áramlását, még mielőtt azok tiltásra kerülnének. Ez az értékes sávszélesség pazarlását jelenti.

Egy kiterjesztett ACL használata megoldást jelent mindkét előbb említett problémára.

Azokra a csomagokra, melyek nem a blokkolt hálózat felé tartanak, nem lesz hatása. A lehetséges hálózati útvonalon található forgalomirányítók soha nem fognak találkozni a tiltott csomagokkal, s ez hozzájárul a sávszélességgel való takarékoskodáshoz.



9.6 A fejezet összefoglalása

- A három rétegű hierarchikus hálózattervezési modellhez való ragaszkodás segíti a hibaelhárítási törekvéseket.
- A hálózati megfigyelő eszközök közé tartoznak többek között: a hálózati segédprogramok, a csomaglehallgató eszközök és az SNMP felügyeleti eszközök.
- Az SNMP lehetővé teszi a hálózaton található különálló eszközök teljesítményének megfigyelését, ügynökök és egy felügyeleti információs adatbázis (MIB) segítségével.
- A konfigurációs állományok biztonsági mentései, a tartalék eszközök vagy a tartalék biztonsági telephelyek lehetővé teszik az összeköttetések gyors helyreállítását.
- Az üzletfolytonossági terv részletezi a biztonsági házirendet és a katasztrófa helyreállítási tervet.
- Egy hálózat hibaelhárításakor határozzuk meg a problémás területeket és határoljuk el a problémát egy adott hibatartományra.

- A kapcsolókhoz társítható leggyakoribb problémák a fizikai rétegben következnek be.
- A LED-ek és a kábeles kapcsolatok szemmel történő leellenőrzése segít a fizikai rétegbeli problémák hibaelhárításában.
- Egy kapcsolón a prioritás értékének megváltoztatásával kikényszeríthető a gyökérponti híd kiválasztása. A gyökérponti hídnak a hálózat központjában kell elhelyezkednie.
- Gondoskodjunk róla, hogy két VTP kiszolgáló legyen egy tartományon belül, a megfelelő tartalék biztosításához.
- Gondoskodjunk arról, hogy minden eszköz amely VLAN információkat oszt meg, ugyanazzal a VTP tartománynévvel rendelkezzen.
- Ellenőrizzük a VTP verziószám információkat és a VTP módot, mielőtt engedélyeznénk egy kapcsolónak a hálózathoz való csatlakozását.
- Számos eszköz létezik a forgalomirányítási problémák hibaelhárításához, ilyenek például az IOS show parancsok, a debug parancsok és a TCP/IP segédprogramok.
- A debug parancsokat csak a hibák körülhatárolására szabad használni, a hálózat normál üzemének figyelésére nem.
- A RIPv1-el kapcsolatos problémák közé sorolhatóak a VLSM támogatás hiányából és a RIPv1 és RIPv2 eszközök kevert használatából adódó problémák.
- Gyakori EIGRP vonatkozású problémák a következők: eltérő AS azonosítószámok, helytelen helyettesítő maszk, automatikus útvonal összefogási problémák nem folytonos alhálózatok esetében.
- Az OSPF problémák nagy része a szomszédsági viszonyok kialakításához és a kapcsolatállapot adatbázisok szinkronizációjához köthető.
- A leggyakoribb fizikai rétegbeli WAN kapcsolódási problémák például a nem megadott órajel vagy a rossz típusú kábel használata.
- Az SLARP hozzárendel egy IP-címet a soros kapcsolat végpontjához, ha a másik végpont már be lett konfigurálva.
- Gondoskodjunk róla, hogy a beágyazás típusa a soros összeköttetés mindkét végén megegyezzen!
- Ha IP-címeket használunk mindkét végpont esetén, akkor azoknak ugyanahhoz a hálózathoz vagy alhálózathoz kell tartozniuk.
- PPP kapcsolódás hibaelhárítása esetében ellenőrizzük, hogy az LCP nyitott állapotban legyen és befejeződjön a hitelesítés és az NCP fázis!
- A fokozott biztonság érdekében használjunk kölcsönös hitelesítést! Az összeköttetés mindkét végpontján ellenőrizzük le, hogy létezzen egy felhasználói fiók a távoli eszköz részére és megfelelően legyen beállítva a jelszó!
- Alapértelmezés szerint, a hitelesítési folyamat során használt felhasználói név, a távoli forgalomirányító neve. Mind a felhasználói név, mind a jelszó érzékenyek a kis és nagybetűkre.

- Az ACL-ek bonyolíthatják a hálózati problémák hibaelhárítását.
- Mindig ellenőrizzük az alapvető hálózati kapcsolódás meglétét, mielőtt alkalmaznánk egy ACL-t!
- Engedélyezzük a naplózást az ACL-ek forgalomra gyakorolt hatásának megtekintéséhez!
- Az ACL-t a megfelelő forgalomirányítóra és interfészre és a helyes irányba kell kell alkalmazni.
- A normál ACL-ek csak egy forrás IP-cím alapján képesek szűrni, így azokat normális esetben a célhoz legközelebb kell elhelyezni.
- Egy kiterjesztett ACL forrás és célcímek, valamint protokollok és portszámok alapján is képes szűrni.
- Egy kiterjesztett ACL forráshoz közeli elhelyezésével letiltható a forgalom, mielőtt az áthaladna a forgalomirányítón vagy átkelhetne a WAN összeköttetésen.
- A rossz interfészen vagy a rossz irányban elhelyezett ACL blokkolhatja azt a forgalmat, amelyet nem szabadna blokkolnia vagy átengedheti azt a forgalmat, amelyet nem szabadna átengednie.

Tartalom

1. Vállalati hálózat....1
1.1 A nagyvállalati hálózatok jellemzői....1
1.1.1 A vállalat üzleti folyamatainak támogatása....1
1.1.2 A forgalom alakulása a nagyvállalati hálózatban....2
1.1.3 Vállalati LAN-ok és WAN-ok....6
1.1.4 Intranetek és extranetek....7
1.2 A vállalati alkalmazások azonosítása....9
1.2.1 Forgalomáramlási mintázatok....9
1.2.2 Alkalmazások és forgalom vállalati hálózaton....9
1.2.3 Prioritások a hálózati forgalomban....11
1.3 Távoli alkalmazottak támogatása....13
1.3.1 Telefonos távmunka....13
1.3.2 Virtuális magánhálózatok....15
1.4 A fejezet összefoglalása....16
2. A vállalatok hálózati infrastruktúrájának megismerése....17
2.1 Az aktuális hálózat leírása....17
2.1.1 A vállalatok hálózati dokumentációja....17
2.1.2 A hálózati szolgáltatási központ....19
2.1.3 A telekommunikációs helyiség kialakításának szempontjai....22
2.2 A vállalati perem támogatása....24
2.2.1 Szolgáltatás-átadás a szolgáltatás-elérési ponton....24
2.2.2 A vállalati határvonal biztonsági szempontjai....25
2.3 Az irányítás és a kapcsolás áttekintése....26
2.3.1 A forgalomirányító....26
2.3.2 A forgalomirányító parancssoros felületének alapvető show parancsai....29
2.3.3 A forgalomirányító alapbeállításainak megadása a parancssoros felületről....30
2.3.4 A kapcsoló....31
2.3.5 A kapcsoló parancssoros felületének parancsai....33
2.4 A fejezet összefoglalása....36
3. Kapcsolás vállalati hálózatokban....37
3.1 A vállalati szintű kapcsolási folyamatok megismerése....37
3.1.1 Kapcsolás és a hálózat szegmentálása....37

3.1.2 Többrétegű kapcsolás 39
3.1.3 Kapcsolási módszerek 40
3.1.4 Kapcsolók védelme 42
3.2 A kapcsolási hurkok kialakulásának megelőzése 43
3.2.1 Redundancia a kapcsolt hálózatokban 43
3.2.2 Feszítőfa protokoll (Spanning tree protocol, STP) 44
3.2.3 Gyökérponti hidak 48
3.2.4 Feszítőfa egy hierarchikus hálózatban 50
3.2.5 Gyors feszítőfa protokoll (Rapid spannig tree protocol, RSTP) 51
3.3 VLAN-ok konfigurálása 52
3.3.1 Virtuális LAN 52
3.3.2 Virtuális helyi hálózat konfigurálása 54
3.3.3 VLAN-ok azonosítása 56
3.4 A trönkölés és VLAN-ok közötti forgalomirányítás 57
3.4.1 Trönkportok 57
3.4.2 Több kapcsolóra kiterjedő VLAN-ok 60
3.4.3 VLAN-ok közötti forgalomirányítás 60
3.5 VLAN-ok kezelése vállalati hálózatokban 63
3.5.1 VLAN trönkprotokoll (VTP) 63
3.5.2 A VTP konfigurálása 65
3.5.3 VLAN-ok az IP-telefónia és a vezeték nélküli hálózatok világában 65
3.5.4 Bevált VLAN megoldások 66
3.6 A fejezet összegzése 67
4. Vállalati hálózatok címzése 69
4.1 IP-hálózatok hierarchikus címzési sémája 69
4.1.1 Egyszintű és hierarchikus hálózatok 69
4.1.2 Hierarchikus hálózati címzés 69
4.1.3 Hálózat felosztása alhálózatokra 70
4.2 A VLSM használata 71
4.2.1 Alhálózati maszk 71
4.2.2 Alhálózat-számítás bináris formában 72
4.2.3 Alapszintű alhálózat-készítés 73
4.2.4 Változó hosszúságú alhálózati maszk (VLSM) 74
4.2.5 VLSM címzés megvalósítása 76

4.3 Az osztály nélküli forgalomirányítás és a CIDR alkalmazása 80
4.3.1 Osztály alapú és osztály nélküli forgalomirányítás 80
4.3.2 CIDR és útvonalösszegzés 82
4.3.3 Az útvonalösszegzés meghatározása 84
4.3.4 Nem összefüggő alhálózatok 84
4.3.5 Alhálózatok létrehozásakor és címzésénél használt bevált módszerek 85
4.4 NAT és PAT használata 86
4.4.1 Privát IP-címtér 86
4.4.2 NAT a vállalati hálózat határán 87
4.4.3 Statikus és dinamikus NAT 88
4.4.4 A PAT használata 90
4.5 A fejezet összefoglalása 91
5. Forgalomirányítás távolságalapú irányító protokollal 92
5.1 Nagyvállalati hálózatok karbantartása 92
5.1.1 Nagyvállalati hálózatok 92
5.1.2 Nagyvállalati hálózati topológiák 93
5.1.3 Statikus és dinamikus forgalomirányítás 95
5.1.4 Statikus útvonalak konfigurálása 97
5.1.5 Alapértelmezett útvonalak 99
5.2 RIP protokollal történő forgalomirányítás 100
5.2.1 Távolságvektor alapú forgalomirányító protokollok 100
5.2.2 Forgalomirányítási információs protokoll (Routing Information Protocol, RIP) 101
5.2.3 RIP konfigurálása 103
5.2.4 A RIP problémái 104
5.2.5 RIP ellenőrzése 105
5.3 Forgalomirányítás az EIGRP protokollal 106
5.3.1 A RIP korlátai 106
5.3.2 Továbbfejlesztett belső átjáró irányító protokoll (EIGRP) 106
5.3.3 EIGRP fogalmak és táblák 108
5.3.4 EIGRP szomszédok és szomszédsági viszonyok 109
5.3.5 EIGRP mértékek és konvergencia 112
5.4 EIGRP megvalósítása 114
5.4.1 EIGRP konfigurálása 114
5.4.2 EIGRP útvonal összevonás 118

5.4.4 Az EIGRP korlátai és problémái 121
5.5 A fejezet összefoglalása 122
6. Kapcsolatállapot alapú forgalomirányítás 123
6.1 OSPF protokollal történő forgalomirányítás 123
6.1.1 Kapcsolatállapot alapú protokoll működése 123
6.1.2 OSPF mérték és konvergencia 124
6.1.3 OSPF szomszédok és szomszédsági viszony 125
6.1.4 OSPF területek 129
6.2 Egyterületű OSPF megvalósítása 130
6.2.1 Egyterületű OSPF alapszintű beállítása 130
6.2.2 Az OSPF hitelesítés beállítása 131
6.2.3 Az OSPF paraméterek beállítása 132
6.2.4 Az OSPF működésének ellenőrzése 134
6.3 Több irányítóprotokoll együttes alkalmazása 136
6.3.1 Alapértelmezett útvonal beállítása és meghirdetése 136
6.3.2 Az OSPF útvonalösszegzés beállítása 137
6.3.3 Az OSPF problémái és korlátai 138
6.3.4 Több protokoll egyidejű alkalmazása nagyvállalati környezetben 139
6.4 A fejezet összefoglalása 141
7. Vállalati WAN kapcsolatok megvalósítása 142
7.1 A vállalati WAN hálózatok összekapcsolása 142
7.1.1 WAN eszközök és technológiák 142
7.1.2 WAN szabványok 145
7.1.3 WAN-kapcsolatok létesítése 146
7.1.4 Csomag- és vonalkapcsolás 147
7.1.5 Helyi hurok és nagytávolságú WAN technológiák 149
7.2 Gyakori WAN beágyazások összehasonlítása 151
7.2.1 Ethernet és WAN beágyazások 151
7.2.2 HDLC és PPP 152
7.2.3A PPP konfigurálása 156
7.2.4 PPP hitelesítés 157
7.2.5 PAP és CHAP konfigurálása 158
7.3 Frame Relay 160
7.3.1 A Frame Relay áttekintése 160

7.3.2 A Frame Rekay működése....161
7.4 A fejezet összefoglalása....164
8. Forgalomszűrés hozzáférési listák használatával....165
8.1 A hozzáférési listák használata....165
8.1.1 Forgalomszűrés....165
8.1.2 A hozzáférés-vezérlési listák....167
8.1.3 Az ACL típusok és használatuk....167
7.1.4 Az ACL feldolgozása....168
8.2 A helyettesítő maszk használata....169
8.2.1 A helyettesítő maszk célja és felépítése....169
8.2.2 A helyettesítő maszk hatásainak elemzése....171
8.3 A hozzáférési listák paraméterezése....174
8.3.1 A normál és a kiterjesztett ACL-ek elhelyezése....174
8.3.2 Az ACL alapbeállításának folyamata....177
8.3.3 A számozott normál ACL beállítása....179
8.3.4 A számozott kiterjesztett ACL beállítása....180
8.3.5 A nevesített ACL beállítása....183
8.3.6 A virtuális terminál alapú hozzáférés beállítása a forgalomirányítón....185
8.4 Meghatározott forgalomtípusok engedélyezése és tiltása....187
8.4.1 ACL-ek beállításának alkalmazása- és portszűrése....187
8.4.2 Az ACL-ek beállítása a kapcsolat-felvétel utáni forgalom támogatásához....188
8.4.3 A NAT és a PAT szerepe az ACL-ek elhelyezésébeb....189
8.4.4 A hálózati ACL-ek és elhelyezésük elemzése....189
8.4.5 Az ACL-ek beállítása a VLAN-ok közötti forgalomirányításhoz....190
8.5 Forgalomszűrés, hozzáférési alkalmazásával....191
8.5.1 A naplózás használata az ACL funkcionalitásának ellenőrzésére....191
8.5.2 A forgalomirányító naplóinak elemzése....192
8.5.3 Bevált ACL megoldások....194
8.6 A fejezet összefoglalása....195
9. Hibaelhárítás egy vállalati hálózaton....197
9.1 A hálózati meghibásodások hatásai....197
9.1.1 Elvárások a vállalati hálózatokkal szemben....197
9.1.2 Nyomon követés és megelőző karbantartás....199
9.1.3 Hibaelhárítás és hibatartomány....201

9.1.4 A hibaelhárítási folyamat 203
9.2 Kapcsolási és kapcsolódási problémák hibaelhárítása 206
9.2.1 Kapcsolók alapvető hibaelhárítása 206
9.2.2 VLAN konfigurációs problémák hibaelhárítása 209
9.2.3 VTP hibaelhárítás 210
9.3 Forgalomirányítási problémák hibaelhárítása 211
9.3.1 RIP forgalomirányítási problémák 211
9.3.2 EIGRP forgalomirányítási problémák 212
9.3.3 OSPF forgalomirányítási problémák 213
9.3.4 Útvonal elosztási problémák 213
9.4 WAN konfigurációs problémák hibaelhárítása 214
9.4.1 WAN kapcsolódás hibaelhárítása 214
9.4.2 WAN hitelesítés hibaelhárítása 216
9.5 ACL-ekkel kapcsolatos problémák hibaelhárítása 217
9.5.1 ACL-ekkel kapcsolatos problémák meghatározása 217
9.5.2 ACL konfigurációs és elhelyezési problémák 218
9.6 A fejezet összefoglalása 219